COMPARTIR SECRETOS SEGUROS USANDO ONETIMESECRET

Versión 1.0

MAIK.ES

Índice

Introducción:

En la era digital, compartir información sensible como contraseñas, claves API, tokens de acceso o instrucciones privada a través de canales habituales como correo electrónico o mensajería instantánea supone un riesgo importante. Los enlaces y mensajes pueden quedar registrados en historiales, copias de seguridad o logs y permanecer accesibles durante mucho tiempo. Herramientas de mensajes de un solo uso como OneTimeSecret ofrecen una alternativa práctica: generan URLs cifradas y efímeras que se eliminan o invalidan tras una única visualización, reduciendo la ventana de exposición.

Este documento explica qué es OneTimeSecret, cómo funciona, presentando una guía práctica para su uso (incluyendo la versión web y la API), analizar ventajas y riesgos, y sugerir alternativas y buenas prácticas.

¿Qué es OnetimeSecret?

OneTimeSecret es un servicio que permite compartir texto sensible mediante enlaces autodestructivos: el remitente crea un "secreto" (texto) que se cifra y se expone mediante una URL única; cuando el destinatario abre esa URL, el secreto se muestra una sola vez y luego se elimina. El servicio está orientado a reducir la permanencia de credenciales en canales inseguros.

¿Cómo funciona técnicamente?

A continuación, explicaré por puntos el funcionamiento de OneTimeSecret:

Creación: El usuario introduce el texto secreto en la interfaz web o envía el contenido a la API. Opcionalmente puede establecer una passphrase o contraseña adicional.

Cifrado: Antes de almacenarse, el secreto se cifra. El servicio guarda sólo el dato cifrado.

Generación de enlace: Se devuelve una URL única que apunta al secreto cifrado.

Acceso y autodestrucción: Cuando el destinatario abre la URL (y proporciona la passphrase si aplica), el servicio descifra el contenido y lo muestra **una sola vez**; tras esta visualización el registro es eliminado, impidiendo posteriores accesos.

Casos de uso recomendados

Tras ver una breve explicación sobre su funcionamiento pasamos a la práctica indicando sus posibles usos recomendados:

Envío puntual de contraseñas temporales.

Compartir claves API o tokens de acceso con colaboradores externos.

Transmitir instrucciones sensibles (por ejemplo, backup keys, instrucciones de emergencia).

Entrega de credenciales temporales a proveedores o integraciones.

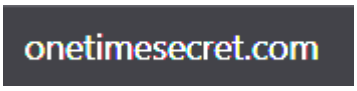
Guía paso a paso, aprende a usar OneTimeSecret

Preparación

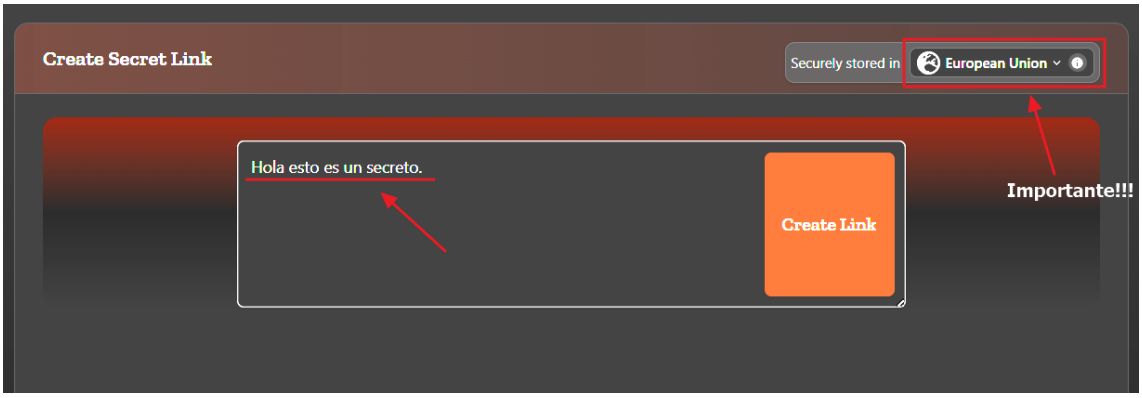
1. Decide el contenido a compartir: que quepa en texto (no es ideal para ficheros grandes).
2. Genera una contraseña adicional (passphrase) fuera del enlace: envíala por otro canal distinto si necesitas mayor seguridad.

Crear un secreto

1. Accede a https://onetimesecret.com.

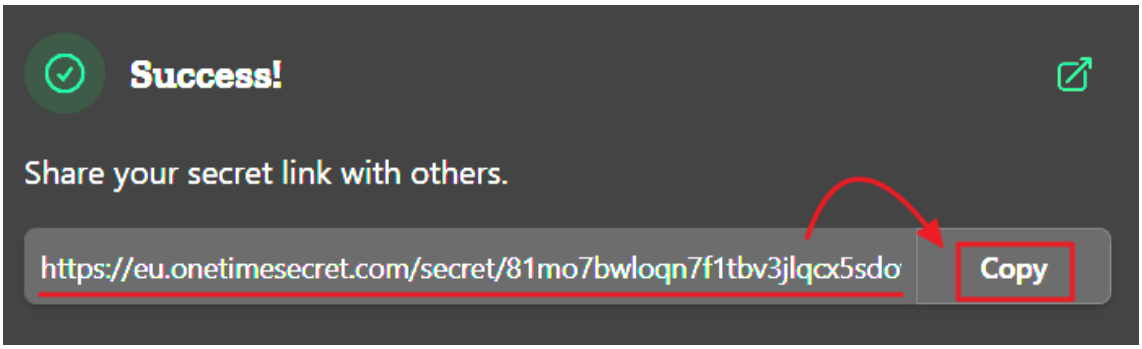


2. Pega o escribe el texto que quieres compartir en el cuadro (muy importante seleccionar el servidor por el cual se quiere enviar dicho secreto ya que según el país las leyes en RGPD pueden cambiar).



3. Haz clic en "Create Link".

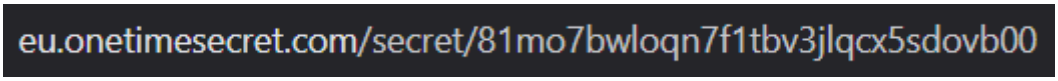
4. Copia la URL generada.



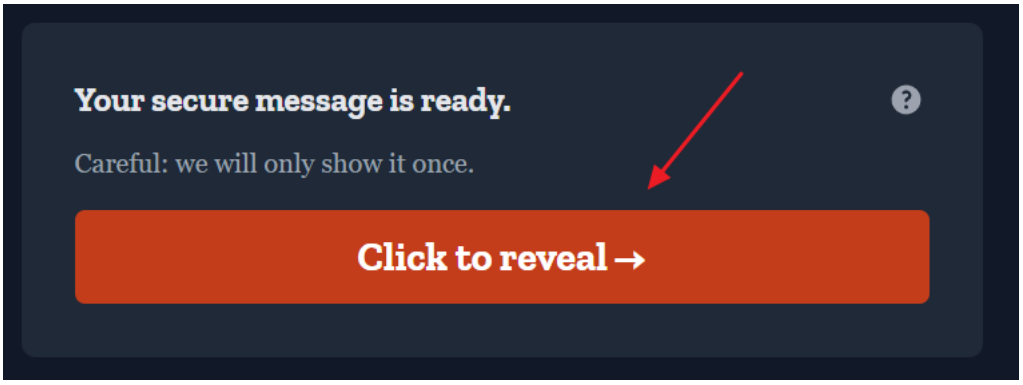
5. Envía la URL al destinatario por un canal como por ejemplo un correo electrónico o una aplicación de mensajería equivalente.

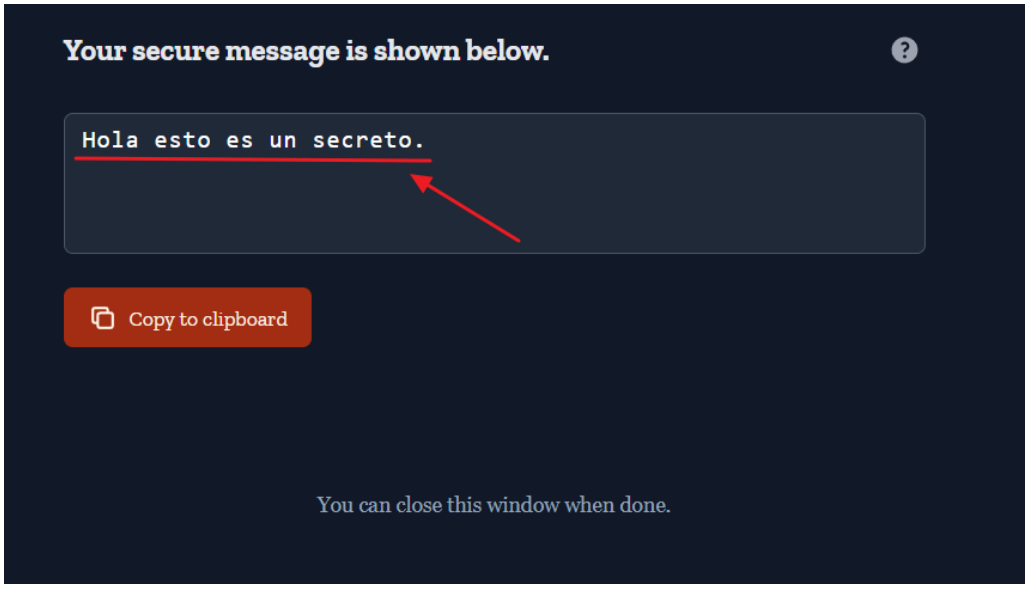
Recepción

1. El destinatario abre la URL.

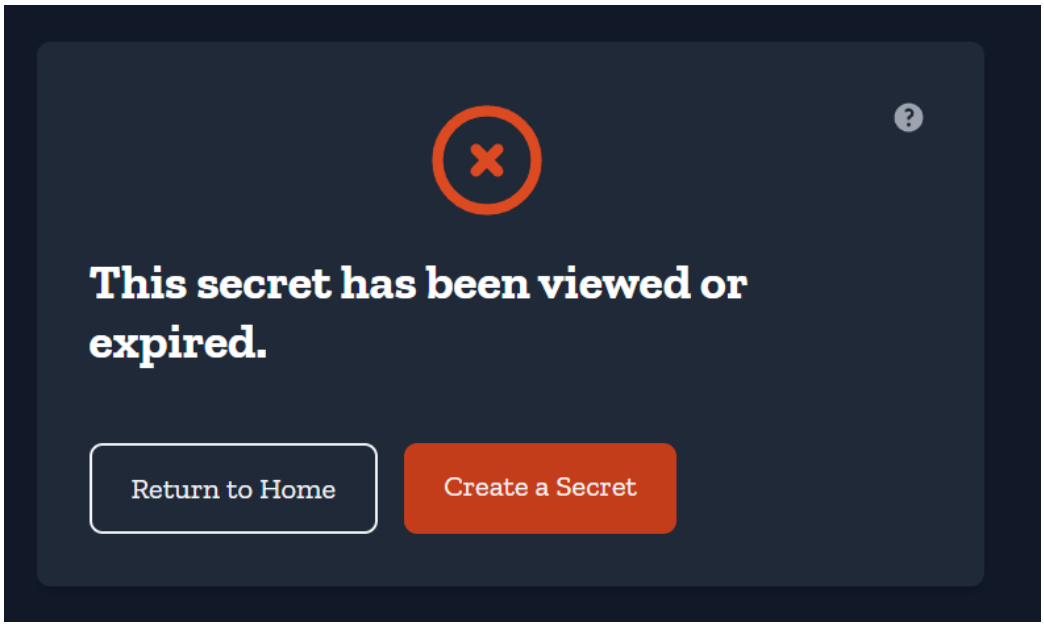


2. Visualiza el secreto (solo una vez).





3. Una vez mostrado, la URL deja de servir: el secreto se autodestruye. Si probamos a recargar la página para visualizarlo de nuevo podemos ver que el secreto ya no es visible.



Buenas prácticas de seguridad al compartir secretos

Canales: Evita utilizar canales de transmisión poco seguros, a poder ser que cuenten con un sistema de cifrado de extremo a extremo.

Auditoría: para usos empresariales, prioriza soluciones que ofrezcan registros/auditoría y control de dominio.

Evitar datos demasiado sensibles: para secretos que requieran cumplimiento usa gestores de contraseñas corporativos o vaults con control de acceso granular.

Limitaciones y riesgos

Una sola capa de protección: la autodestrucción reduce la ventana de exposición, pero no impide que el destinatario haga capturas de pantalla, copie o redistribuya el secreto.

Confianza en el proveedor: usar un servicio público implica confiar en sus prácticas de seguridad y continuidad. Para datos críticos se recomienda self-hosting.

No es un reemplazo completo de un password manager: para gestión a largo plazo de credenciales, use soluciones dedicadas (gestores de contraseñas y vaults).

Otras plataformas similares para utilizar como alternativa

A modo orientativo, existen múltiples alternativas y proyectos afines, tanto servicios SaaS como soluciones auto-hospedadas. Entre ellas se encuentran:

- **PrivateBin / PrivateBin.info** (self-hosted, cifrado de extremo a extremo en cliente).
- **Yopass** (servicio/plataforma con enfoque similar).
- **Privnote.**
- **PasswordPusher / pwpush.**
- **Pastebin** (no diseñado específicamente para secretos, usar con precaución).
- **Otras soluciones modernas:** vanish.so, scrt.link, dele.to.

Conclusión

Compartir secretos por canales tradicionales conlleva riesgos evitables. Herramientas como OnetimeSecret proporcionan una forma sencilla y efectiva de reducir la persistencia de información sensible mediante enlaces efímeros y cifrado. Para un uso responsable, combínalas con buenas prácticas (canales separados, passphrases, TTL) y, cuando el dato sea crítico, considere opciones de self-hosting o gestores profesionales de secretos.