

PASSWORDLESS AUTHENTICATION SYSTEMS

SEGURIDAD Y EXPERIENCIA DE USUARIO EN LA ERA POST-PASSWORD



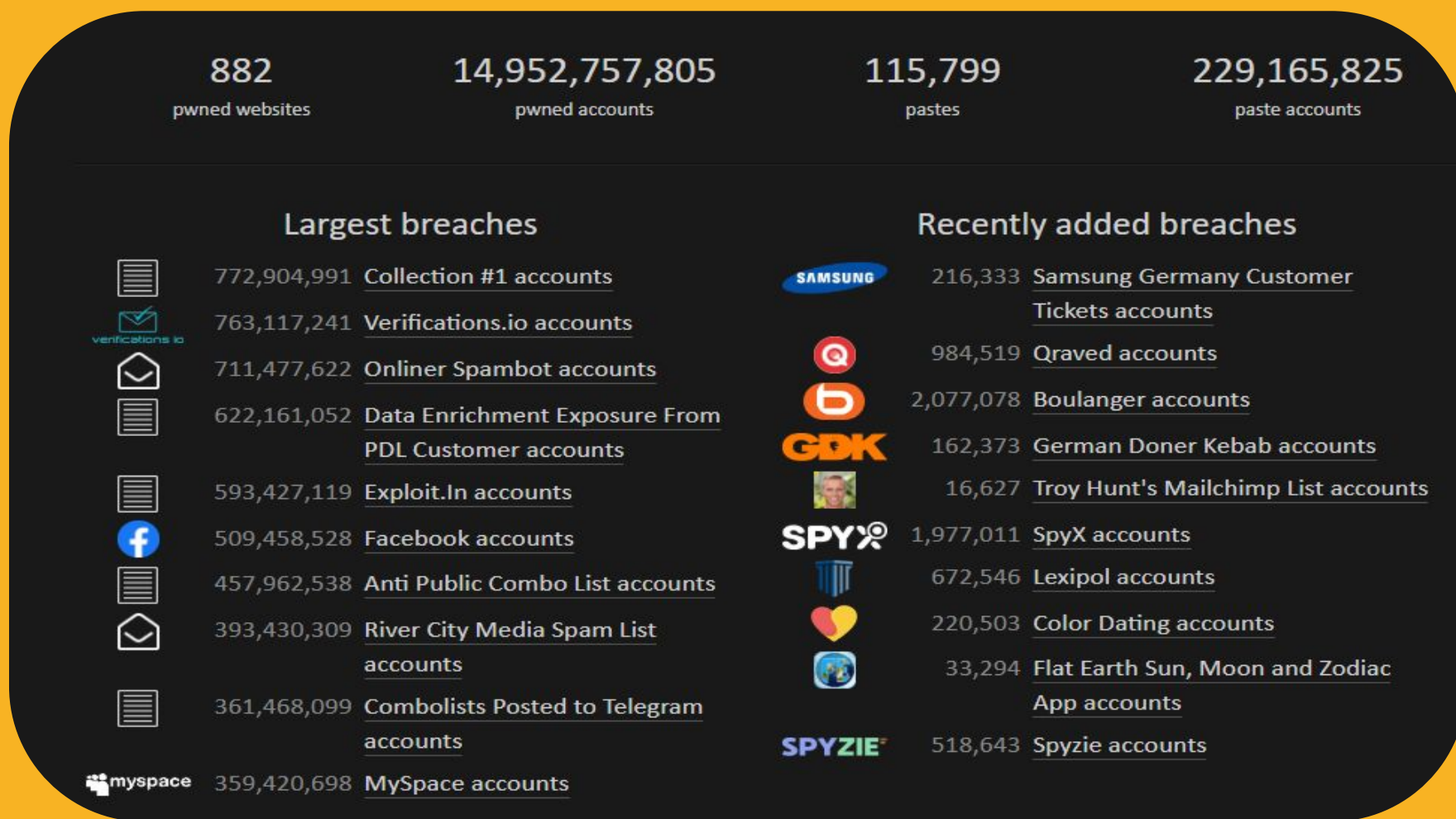
Alfonso-Fernando Cano Pérez

Aleix Padrell Gondolbeu

Àlex Ollé Parcerisas



INTRODUCCIÓN



¿CÓMO INFORMÁTICOS, SOMOS SEGUROS?



¿QUÉ ES LA AUTENTICACIÓN SIN CONTRASEÑAS?

Un enfoque de seguridad que **elimina el uso de contraseñas** tradicionales, reemplazándolas por métodos más seguros y cómodos como biometría, tokens o notificaciones push.



¿POR QUÉ CAMBIAR EL MODELO ACTUAL?

- Las contraseñas son **difíciles de recordar**.
- Muchos usuarios **reutilizan** las mismas claves.
- Son **vulnerables** a ataques como phishing y fuerza bruta.
- La **experiencia de usuario** suele ser **frustrante**.



VENTAJAS DEL MODELO PASSWORDLESS

- **Seguridad mejorada:** reduce riesgos de ataques comunes.
- **Mejor experiencia de usuario:** más rápido y cómodo.
- **Menor coste de soporte:** menos restablecimientos de contraseñas.
- **Mayor cumplimiento normativo:** alineado con estándares modernos.





MÉTODOS PASSWORDLESS

BIOMETRÍA

Basado en características fisiológicas del usuario como huellas dactilares, patrones faciales, reconocimiento de iris o VOZ.

Ventajas:

- Características únicas del usuario (no se pueden suplantar fácilmente)
- Experiencia de usuario sencilla
- No se requieren elementos externos (no se pueden perder, robar, ...)
- Identificación unipersonal

Inconvenientes:

- Riesgos de privacidad: En caso de ser suplantado, no se puede restablecer
- Falsos positivos /negativos

Aplicaciones:

- Desbloqueo dispositivos móviles
- Control de acceso
- Transacciones bancarias



AUTENTICACIÓN MEDIANTE DISPOSITIVO EXTERNO

Basado en dispositivos que almacenan claves criptográficas privadas y requieren una confirmación por parte del usuario

Ventajas:

- Evitan el phishing (no se pueden interceptar)
- Funcionan sin acceso a internet
- Necesidad de elemento + PIN para autenticar.

Inconvenientes:

- Requieren llevar un dispositivo o elemento con las claves criptográficas
- No tan cómodo como otros métodos

Aplicaciones:

- YubiKey para logins en webs (usa NFC y USB-C)
- Pares de llaves FIDO2



CREDENCIALES BASADAS EN PKI

Basado en claves asimétricas privadas que se almacenan en un chip seguro. La autenticación se usa mediante firma digital

Ventajas:

- Alta seguridad debido a la longitud de las claves
- Escalable (Puedes generar infinitos certificados)

Inconvenientes:

- Complejo de gestionar (requiere infraestructura especializada)
- Coste elevado
- Requiere elemento externo

Aplicaciones:

- Firma de documentos con DNI-e
- Acceso remoto seguro (VPNs)



PASSKEYS Y AUTENTICACIÓN FIDO2 SIN DISPOSITIVOS EXTERNOS

Basado en credenciales FIDO2 almacenadas en el gestor de contraseñas del sistema operativo. Permiten la sincronización entre dispositivos

Ventajas:

- Sincronización multiplataforma
- Recuperación simplificada
- Sencillo e invisible al usuario

Inconvenientes:

- Problemas de compatibilidad entre ecosistemas
- Brechas de seguridad pueden comprometer el acceso a múltiples plataformas

Aplicaciones:

- Autenticación sin contraseña en aplicaciones móviles
- Inicio de sesión en sitios web.
- OAuth y otros servicios centralizados



AUTENTICACIÓN MÓVIL PUSH Y OTP

Basado en notificaciones a una aplicación móvil, donde el usuario aprueba el acceso.

Ventajas:

- Fácil de implementar
- Compatible con cualquier dispositivo
- Difícil de suplantar debido a volatilidad

Inconvenientes:

- Dependiente de otros servicios y de la red
- Vulnerable al SIM swapping
- Menos usable que otros métodos

Aplicaciones:

- Acceso a sistemas críticos
- Autorización a herramientas avanzadas
- Autenticación en 2 pasos
- Google Authenticator o Microsoft Authenticator





OTP (ONE TIME PASSWORD)

Análisis en profundidad



El debate se realizará sobre este apartado

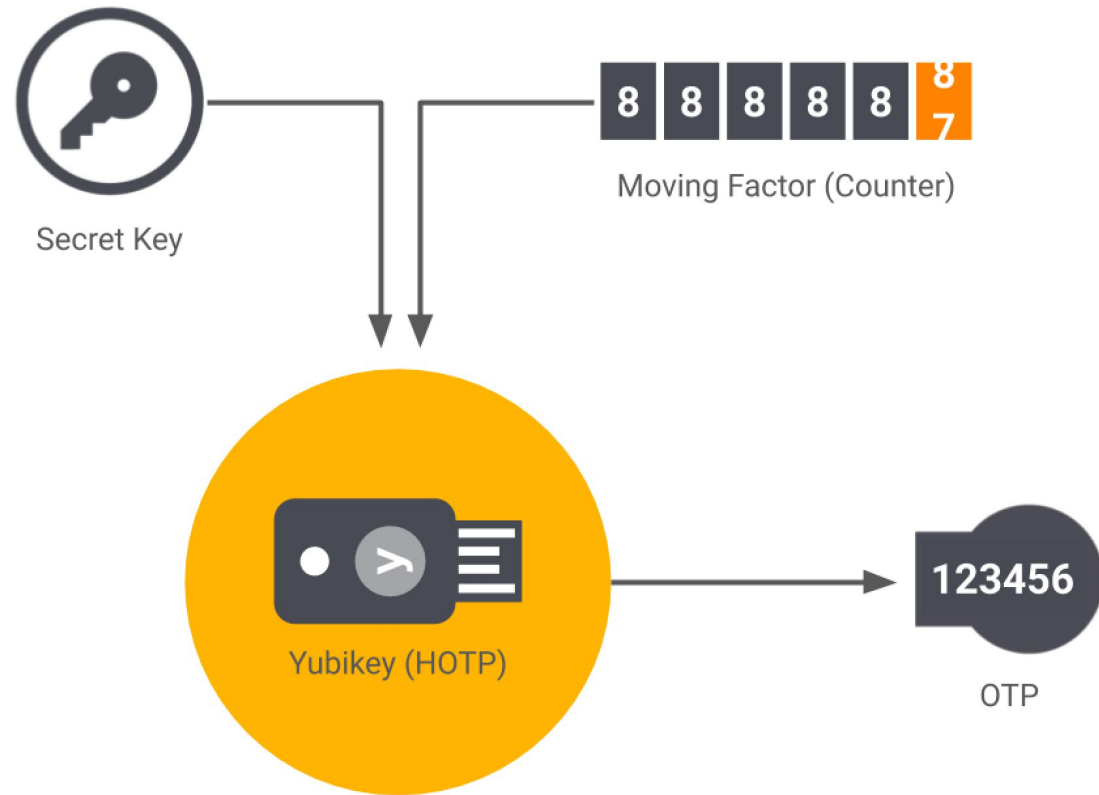
¿QUÉ ES OTP?

- Contraseña de un solo uso
- Validez limitada en el tiempo
- No puede reutilizarse



TIPOS DE OTP

HOTP

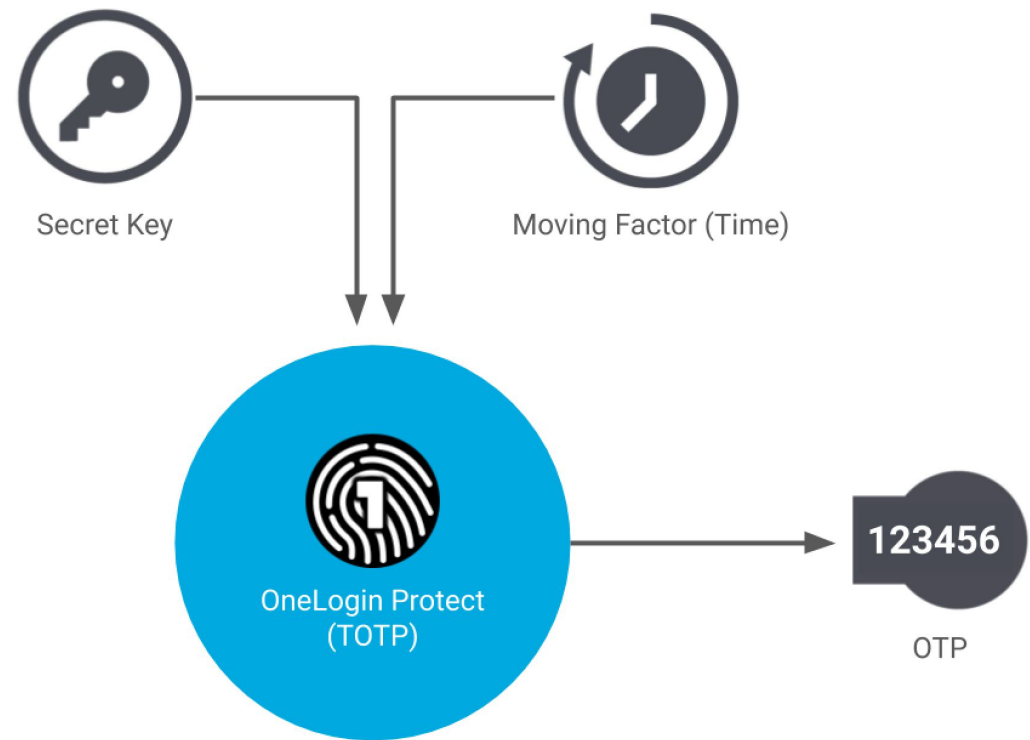


Source: <https://www.onelogin.com/learn/otp-totp-hotp>

HOTP

- Basada en un **contador** incremental
- No depende del tiempo, útil si la sincronización horaria es un problema.
- Susceptible a ataques de **fuerza bruta**, ya que el código no caduca hasta que se usa.

TOTP



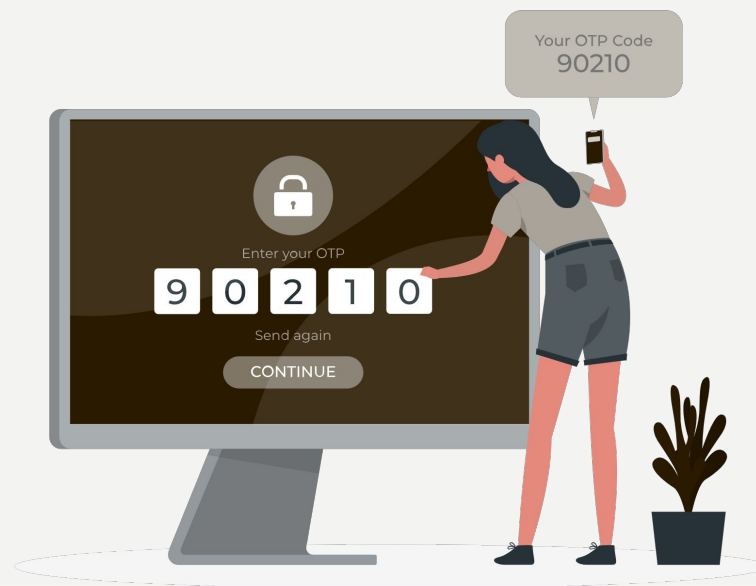
Source: <https://www.onelogin.com/learn/otp-totp-hotp>

TOTP

- Basada en el **tiempo**, el código cambia cada 30-90 segundos.
- Más segura frente a ataques de fuerza bruta, ya que el código expira rápidamente.
- Puede causar problemas si hay desfase horario entre el servidor y el dispositivo del usuario.

TIPOS DE ENVÍO OTP

- SMS
- Email
- Messaging apps
- Hardware keys
- Authenticator apps



VENTAJAS

- Mayor seguridad
- Fáciles de usar
- Versatilidad

INCONVENIENTES

- Dependencia de la entrega
- Vulnerabilidades
- Secretos compartidos



FUTURO DE OTP

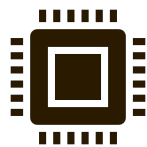
- Integración con biometría
- Autenticación sin contraseñas (passwordless)
- Inteligencia artificial y machine learning

FUTURO DE LA AUTENTICACIÓN

¿FUTURO O PRESENTE?



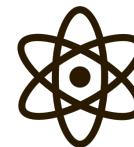
A finales de 2025, se estima que el 65 % de las plataformas y aplicaciones contarán con algún sistema passwordless como método primario de acceso.



Para 2030, el 90% de las aplicaciones ofrecerán passkeys como opción predeterminada de autenticación y el e-commerce realizarán el checkout mediante reconocimiento facial.



Auge de la biometría para sectores críticos como la aviación, laboratorios y centrales nucleares.



Desaparición de tokens físicos



Integración con Realidad Aumentada

TECNOLOGÍAS EMERGENTES EN AUTENTICACIÓN PASSWORLESS

Inteligencia Artificial y Machine Learning Adaptativo

Criptografía Post-Cuántica

Identidades Descentralizadas (SSI - Self-Sovereign Identity)

Biometría Comportamental y Continua

TENDENCIAS DE MERCADO Y ADOPCIÓN EMPRESARIAL

Crecimiento Exponencial en Sectores Regulados

Convergencia con Arquitecturas Zero-Trust

Expansión de Ecosistemas Passwordless

Regulaciones como Motor de Cambio


DESAFÍOS CRÍTICOS Y CONSIDERACIONES FUTURAS



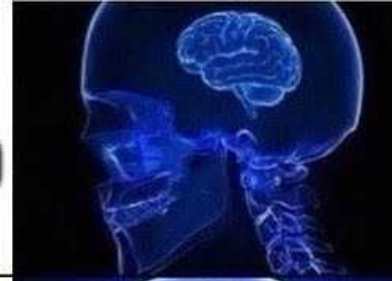
CONCLUSIONES

- Los sistemas Passwordless son una necesidad
- Ofrecen una seguridad mejor si se usan correctamente
- Cada vez más empresas deciden implantarlos
- Como desarrolladores, tenemos el reto de aprender a implementarlos
- Mejoran la experiencia de usuario
- No hay una metodología perfecta, sino que cada una tiene un propósito

PREGUNTAS Y DEBATE

- ¿Cuál es vuestra experiencia con OTP? (por ejemplo, con aplicaciones de bancos)
 - ¿Creéis que es más seguro que un sistema tradicional?
 - ¿Es OTP realmente passwordless o simplemente una contraseña temporal?
 - ¿Debería una empresa obligar a sus usuarios a usar OTP o dar varias opciones?
- 

**USERNAME +
EASY PASSWORD**



**USERNAME
+ STRONG
PASSWORD**



**USERNAME +
PASSWORD & OTP**



**USERNAME + PASSWORD
&
OTP & OTHER MFA**

