Full Duplex Authentication®

Mitigación del phishing y de ataques Browser-in-Browser y de proxy malicioso

Este informe presenta Full Duplex Authentication®, una tecnología de seguridad diseñada para afrontar las crecientes amenazas de phishing, de navegador dentro del navegador y de proxy malicioso. Para comprender Full Duplex Authentication®, primero analizaremos estas amenazas y después el enfoque innovador de la patente estadounidense 11,245,526.

Introducción

La seguridad en línea es esencial ante la evolución de las amenazas digitales. El phishing y los ataques Browser-in-Browser y de proxy malicioso son métodos que los actores maliciosos emplean para comprometer credenciales e información confidencial. Full Duplex Authentication® se presenta como una solución robusta para contrarrestarlos.

¿Qué es la autenticación?

La autenticación verifica una identidad digital en línea. Cuando una persona se vincula con una identidad digital, se le solicitan credenciales para demostrar que es quien afirma ser.



Tres métodos habituales de validación:

- El primero es algo que el usuario sabe: una contraseña, un número de identificación personal (PIN) o un código de un solo uso (OTP).

• El segundo es algo que el usuario posee, como un dispositivo registrado, un token digital en ese dispositivo o un equipo físico específico, como una YubiKey.
• El tercero es algo que el usuario es: un rasgo biométrico como el rostro o la huella digital. Si el usuario realiza más de una acción de verificación, se denomina autenticación multifactor (MFA). Para garantizar el máximo nivel de seguridad al autenticar una identidad digital, los tres métodos deberían aplicarse cada vez que el usuario accede a un sistema o servicio.

Amenazas contra la autenticación

La ingeniería social y el phishing causan 70 % a 90 % de las brechas maliciosas.

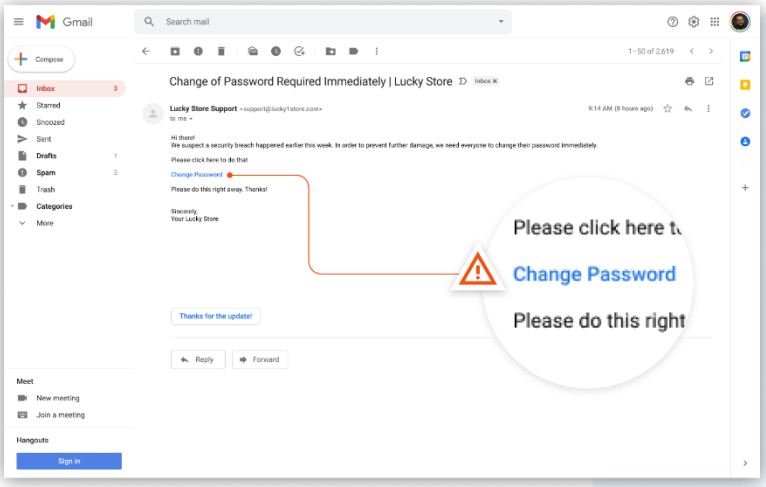
Fuente: KnowBe4

Durante años, los atacantes han centrado sus ciberataques en robar credenciales de acceso en línea.

Según el informe Verizon DBIR, en 2023 el 74 % de las brechas de seguridad involucró el factor humano, incluidos ataques de ingeniería social como el phishing.

Obtener las credenciales mediante ingeniería social se ha vuelto más fácil para los atacantes que ejecutar sofisticados ataques de fuerza bruta.

Estos son algunos métodos frecuentes para obtener credenciales de forma fraudulenta y eludir la autenticación multifactor:

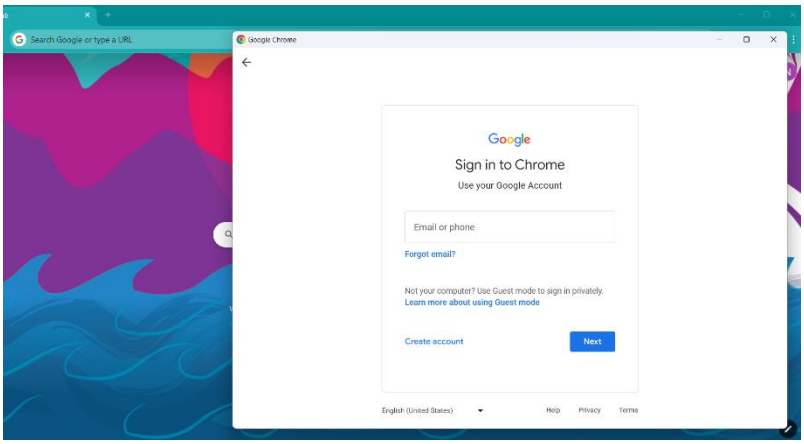


• Phishing: intentos fraudulentos de obtener información confidencial haciéndose pasar por una entidad de confianza. Suele propagarse mediante correos o sitios falsos y explota la psicología humana para inducir a revelar datos. Incluye el smishing, por mensajes de texto, y el vishing, que ataca los restablecimientos de contraseña enviados por correo de voz. El quishing usa códigos QR para atraer a la víctima. El phishing suele combinarse con correos y sitios que suplantan identidades.

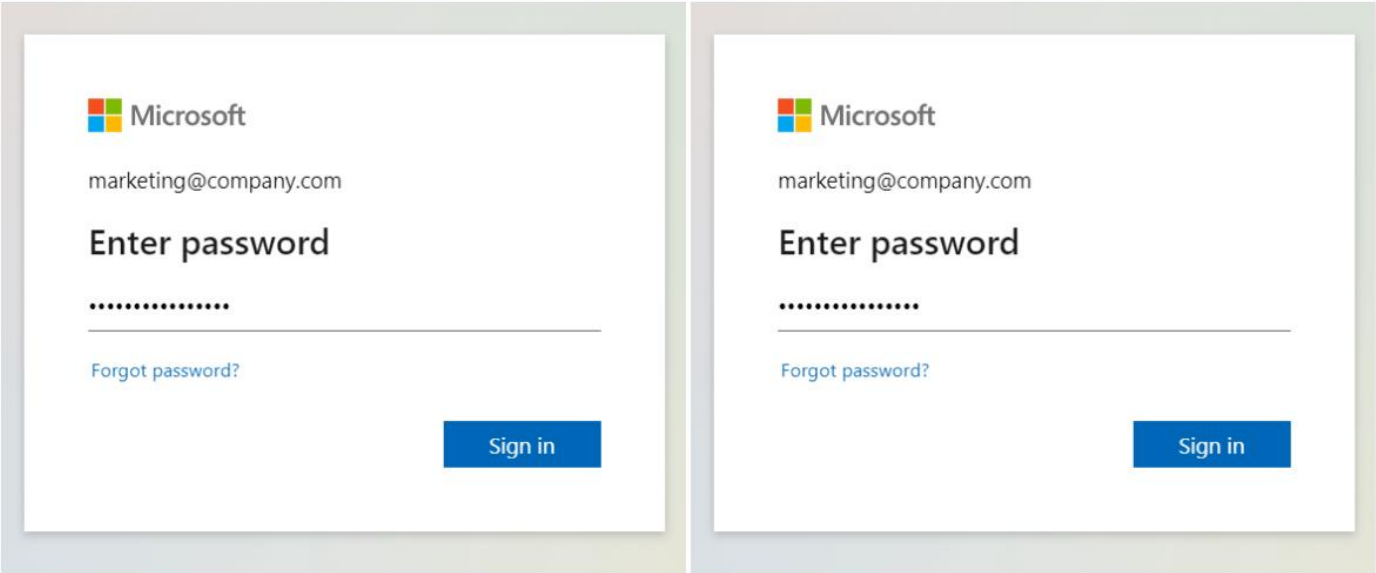
El usuario recibe un correo falso que parece proceder de una organización legítima, como

un banco, una empresa de telecomunicaciones o Amazon, Microsoft, Apple o Google. El correo indica un problema con la cuenta y pide iniciar sesión. Al pulsar el enlace, el usuario puede no advertir que la URL no corresponde al sitio esperado. Cuando introduce sus credenciales, la cuenta queda comprometida.

• Ataques Browser-in-Browser: una entidad maliciosa inyecta código en un sitio legítimo y compromete la seguridad del navegador. Puede robar información confidencial o ejecutar acciones no autorizadas en nombre del usuario. El ataque es difícil de detectar: el usuario puede no advertir el cambio de URL porque los diálogos de navegador dentro del navegador no muestran una URL. Al introducir las credenciales, la cuenta queda comprometida.



• Ataques de proxy malicioso: interceptan la comunicación entre el usuario y el servidor web mediante servidores proxy maliciosos. Los atacantes pueden interceptar datos confidenciales, manipular la comunicación y robar la contraseña durante el inicio de sesión.



¿Puedes identificar cuál es falso?

Acerca de Full Duplex Authentication®

Aunque se abandonaran los métodos basados en conocimientos, no se impedirían los ataques actuales de phishing e ingeniería social. Según este informe, los métodos de autenticación tienen una debilidad fundamental: el flujo de verificación es unidireccional. El servicio solicitante desafía al usuario a realizar las acciones necesarias para demostrar su validez.

El usuario también debe poder exigir que el servicio de autenticación demuestre su validez. De lo contrario, los atacantes pueden suplantar un servicio legítimo para obtener una contraseña, un token digital o una verificación biométrica del dispositivo. Identité® desarrolló y patentó Full Duplex Authentication® para abordar esta debilidad. La patente estadounidense 11,245,526 describe una autenticación con comunicación bidireccional cifrada entre el usuario y el sistema. Frente a la autenticación unidireccional convencional, Full Duplex Authentication® mantiene un intercambio continuo y dinámico de información durante todo el flujo de autenticación.

¿Cómo funciona Full Duplex Authentication®?

Un servidor de autenticación llamado NoPass™ por Identité, abreviatura de «sin contraseña», establece una relación segura con un servicio de terceros. El servicio recopila la identificación del usuario e inicia la autenticación. Puede ser Microsoft AD o Azure, herramientas SSO como Okta, una VPN, Citrix u otra aplicación o portal que requiera autenticación. NoPass™ ofrece varias vías de integración. • SSO federado: el servidor NoPass™ actúa como proveedor de identidad para Microsoft Azure/AD u otras herramientas SSO, como Okta, PingIdentity o KeyCloak. • RADIUS: el servidor NoPass™ se configura como cliente RADIUS.



• API: el servidor NoPass™ establece comunicaciones seguras con portales web y aplicaciones móviles.

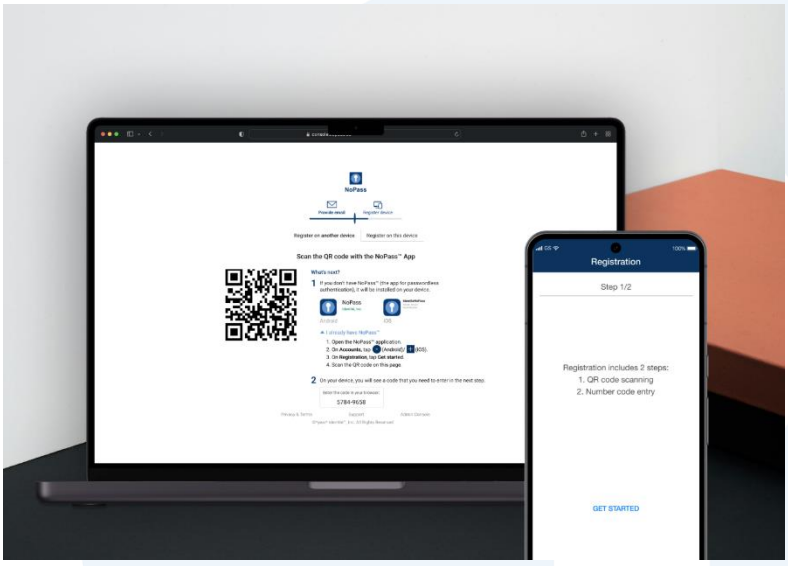
El servidor NoPass™ interactúa con el usuario mediante aplicaciones para iOS, Android, Windows y macOS, disponibles en tiendas públicas, normalmente al registrarse por primera vez. La aplicación recibe notificaciones push seguras cuando se solicita autenticación a un servidor de terceros configurado para usar NoPass™ Full Duplex Authentication®. Contiene credenciales únicas para cada portal o servicio registrado. Están cifradas y no pueden reutilizarse para acceder al servicio, por ejemplo mediante un ataque de repetición. Los usuarios pueden respaldarlas y sincronizarlas con otros dispositivos si la política de seguridad lo permite.

Registro en Full Duplex Authentication®

Para registrarse, el usuario se autentica mediante el flujo nativo del servicio, normalmente con nombre de usuario y contraseña. Tras verificarse la autenticación, se le dirige a la interfaz de registro de Full Duplex Authentication®. En el registro participan el usuario y un dispositivo, como una PC, una Mac o un teléfono inteligente.

Según la política de seguridad del servidor de autenticación NoPass™, el usuario elige el dispositivo e instala una pequeña aplicación. Esta almacena una credencial Full Duplex Authentication® por cada cuenta del usuario en cada servicio registrado. Se admiten varias cuentas para un mismo servicio.

La interfaz de registro permite escanear un código QR o pulsar «Continuar», lo que abre una instalación local de la aplicación Full Duplex Authentication®.

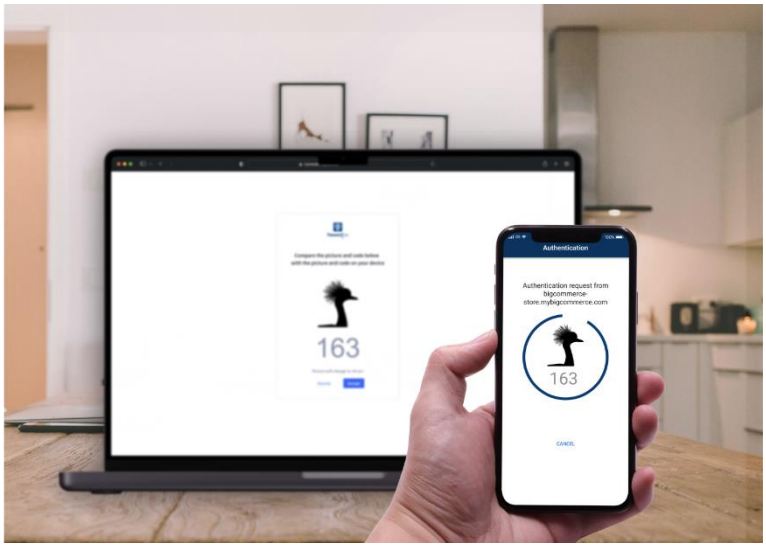


Si la aplicación se instala en un dispositivo distinto del que muestra el registro, se solicita confirmar un código de ocho dígitos para demostrar la posesión del segundo dispositivo. Tras confirmar el registro, el usuario queda autenticado y vuelve al servicio para continuar su tarea. Cuando cierra sesión y regresa, no se le solicita una contraseña: se le guía por el flujo de Full Duplex Authentication®.

La aplicación Full Duplex Authentication® reconoce y utiliza los factores adicionales disponibles en el dispositivo, como biometría o tokens físicos YubiKey. También puede configurarse un PIN. Estos factores adicionales mitigan los riesgos en caso de pérdida o robo del dispositivo.

Flujo de uso de Full Duplex Authentication®

El usuario puede elegir uno o dos dispositivos. El uso de dos ofrece mayor seguridad: uno muestra el diálogo de acceso y otro, con la aplicación de autenticación, recibe y acepta la notificación push. El usuario inicia el acceso introduciendo su nombre en el primer dispositivo. El nombre se envía a NoPass. Si está registrado, NoPass envía instrucciones al portal registrado. Al introducir el nombre de usuario, aparecen una imagen y un número en el dispositivo de autenticación registrado.



Full Duplex Authentication® se completa cuando la aplicación del dispositivo registrado autentica al servidor y acepta el mensaje para mostrar la imagen y el número. Al aceptar las credenciales del servidor, la aplicación descifra y reconstruye la misma imagen y número en el dispositivo de autenticación. Ambos cambian cada 30 segundos; el proceso se repite hasta que el usuario responde. La configuración de NoPass puede limitar los intentos para impedir la aceptación accidental de una notificación push por fatiga. El usuario también puede rechazar un acceso que no haya iniciado.

Antes de confirmar a NoPass la validez de las credenciales, pueden ejecutarse factores adicionales, como verificar un token físico YubiKey o una prueba biométrica. Las opciones dependen del dispositivo y sus capacidades. Por ejemplo, los teléfonos iPhone y Android incorporan reconocimiento facial y de huellas digitales.

También puede exigirse una YubiKey para proteger una máquina virtual o una estación compartida. Tras la comprobación local, la aplicación envía

las credenciales al servidor NoPass. Si son válidas, NoPass indica al servidor de terceros o portal web que permita al usuario entrar en la aplicación.

Full Duplex Authentication® previene ciberataques comunes

La mayoría de los ciberataques implica robar credenciales. Las organizaciones han avanzado en herramientas que impiden aprovechar malware sofisticado y vulnerabilidades conocidas. Por ello, los atacantes han recurrido a herramientas y métodos menos sofisticados, dirigidos al eslabón más débil de la seguridad: las personas.

Full Duplex Authentication® aporta protección adicional frente a ataques de ingeniería social porque el servicio solicitante siempre debe autenticarse ante el usuario. Estos son algunos ataques y la forma en que Full Duplex Authentication® los contrarresta.

- Prevención del phishing: Full Duplex Authentication® introduce desafíos dinámicos y respuestas durante todo el proceso. La interacción en tiempo real entre el usuario y el servidor reduce la eficacia del phishing: las credenciales estáticas, como contraseñas o tokens, no bastan por sí solas para autenticarse correctamente.

- Mitigación de Browser-in-Browser: la comunicación bidireccional de Full Duplex Authentication® permite verificar constantemente la legitimidad del navegador. Los intentos de inyección de código o manipulación no autorizados se detectan rápidamente, impidiendo ataques de navegador dentro del navegador.
- Resistencia a proxies maliciosos: Full Duplex Authentication® verifica de forma constante la autenticidad y el origen del canal de comunicación. Esta resistencia frustra las tácticas de los proxies maliciosos e impide la interceptación y manipulación no autorizadas de datos.

Impacto empresarial

Como señala Verizon DBIR 2023, la mayoría de las brechas de datos se produce a través de personas, el eslabón más débil de la cadena de seguridad.

Además de las posibles pérdidas por accesos no autorizados, existen costos operativos asociados a la autenticación multifactor basada en contraseñas y

En 2023, el costo medio de una brecha de datos fue de 4,5 millones de USD.

Fuente: IBM

dispositivos físicos. Por los riesgos de las contraseñas, deben cambiarse periódicamente; la práctica recomendada citada propone cada 90 días. Esto puede costar a una organización hasta una hora de trabajo por contraseña al año.

Si un dispositivo MFA se pierde o falla, sustituirlo aumenta los costos operativos. Las aplicaciones Full Duplex Authentication® pueden instalarse en un dispositivo que el empleado ya posee. La aplicación realiza al menos dos factores de autenticación, lo que reduce de forma significativa los costos asociados a otras herramientas MFA.

Conclusión

Ante amenazas cambiantes, son esenciales las medidas innovadoras. Full Duplex Authentication®, descrita en la patente estadounidense 11,245,526, se sitúa a la vanguardia de la autenticación moderna y ofrece una defensa dinámica y robusta frente al phishing, los ataques Browser-in-Browser y los proxies maliciosos.

Implementar esta tecnología innovadora y galardonada es fundamental para proteger la integridad y confidencialidad de las interacciones en línea en un entorno digital cambiante.

Full Duplex Authentication® permite eliminar las contraseñas del flujo de autenticación. Esto simplifica el proceso y reduce los costos operativos de gestión de contraseñas.

> Visita el sitio de Identité para conocer nuestras soluciones MFA. Síguenos en LinkedIn para recibir noticias sobre seguridad y gestión de identidades. Contacta a Ventas para solicitar demostraciones.