yubico

Proteja los servicios financieros con una MFA moderna y resistente al phishing

El sector de los servicios financieros sufre constantes ciberataques

Uno de los principales objetivos de los ciberdelincuentes es el sector de los servicios financieros, en el que una filtración de datos puede llegar a costar una media de 5,90 millones de dólares.[1] En este sector, las empresas se enfrentan a un doble reto en materia de ciberseguridad: por un lado, las amenazas de phishing dirigidas a los empleados; por otro, los intentos de apropiación de cuentas en plataformas móviles y virtuales de clientes de banca comercial y minorista.

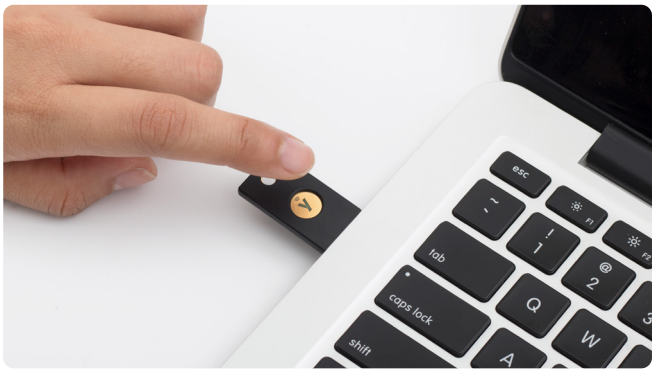
No todos los tipos de MFA son iguales

El sector de los servicios financieros fue uno de los primeros en adoptar la autenticación móvil, por ejemplo, mediante SMS, OTP y notificaciones push. Sin embargo, aunque cualquier tipo de autenticación de múltiples factores (MFA) es mejor que una simple contraseña, no todos los sistemas son iguales. Como ya hemos dicho, las contraseñas no ofrecen mucha protección, y la MFA basada en preguntas de seguridad, códigos enviados por SMS, OTP y notificaciones push es vulnerable ante las suplantaciones de SIM y los ataques de phishing y de intermediarios. Los autenticadores móviles tampoco ofrecen la mejor experiencia de usuario.

Una MFA resistente al phishing puede formar una férrea primera línea de defensa para las empresas de servicios financieros, ya sea para proteger los activos de la compañía o de los clientes.

¿Qué es la MFA resistente al phishing?

Los sistemas de MFA resistentes al phishing se basan en la verificación criptográfica entre dispositivos o entre el dispositivo y un dominio, lo que los hace inmunes a los intentos de comprometer o subvertir el proceso de autenticación. Según la publicación especial (Special Publication o SP) 800-63 del Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology o NIST), solo dos tipos de autenticación cumplen actualmente los requisitos para una MFA resistente al phishing: PIV/Smart Card y el moderno estándar de autenticación FIDO2/WebAuthn.



YubiKey: Un sistema de MFA moderno, resistente al phishing y sin contraseña

Para reducir el phishing a escala empresarial y la apropiación de cuentas de clientes, Yubico presenta la YubiKey, que permite una autenticación de múltiples factores segura, sencilla y sin contraseña.

En investigaciones independientes se ha demostrado que las YubiKeys ofrecen los niveles más altos de seguridad contra la apropiación de cuentas, lo que evita los ataques dirigidos y proporciona un retorno de la inversión del 203 %.[2]

Riesgo de robo de cuentas

0%
Llave de seguridad (YubiKey)

10%
Mensaje en dispositivo

24%
Código por SMS

21%
Correo electrónico secundario

50%
Número de teléfono

Investigación de Google, NYU y UCSD basada en 350 000 intentos reales de secuestro. Los resultados mostrados se corresponden con ataques dirigidos.

Las YubiKeys son idóneas tanto para personal de oficina como para los empleados que trabajan de forma remota o híbrida; se pueden usar en entornos con restricciones para móviles, en estaciones de trabajo y dispositivos compartidos, así como para prestar servicios digitales orientados al cliente. Del mismo modo, son una alternativa para aquellos usuarios que no utilizan la autenticación móvil o que no pueden o no quieren utilizarla. Gracias a su compatibilidad multiprotocolo (Smart Card, OTP, OpenPGP, FIDO U2F y FIDO2/WebAuthn), son fáciles de implementar y usar: una sola YubiKey vale para identificarse en diferentes aplicaciones, servicios y dispositivos, ya sean antiguos o modernos, lo que permite adoptar fácilmente un moderno sistema de autenticación sin contraseña.

Las YubiKeys también cumplen el FIPS 140-2 conforme al nivel 3 de garantía de autenticador (AAL3) según la SP 800-63B del NIST. Asimismo, garantizan el cumplimiento de la ley SOX, la normativa PCI DSS 4.0, la Directiva PSD2, el GDPR y la Circular 2022-04 de la Oficina para la Protección Financiera del Consumidor (CFPB, por sus siglas en inglés).

Casos de uso habituales en el sector financiero que pueden resolverse con la YubiKey

1. Proteger a los empleados que trabajan de forma remota o híbrida

La MFA resistente al phishing debería ser uno de los principales requisitos de las políticas de trabajo remoto e híbrido. Las YubiKeys proporcionan la MFA más segura y se integran fácilmente en los sistemas e infraestructuras existentes, incluidos los sistemas de gestión de identidades y accesos como Microsoft, Okta, Duo, Ping y Hypr. Con la YubiKey, las empresas de servicios financieros pueden garantizar que los empleados que trabajan de forma remota e híbrida accedan de forma segura a los ordenadores, a las VPN y a los programas de gestión de contraseñas, independientemente de su ubicación. Las YubiKeys pueden utilizarse incluso para generar de forma segura códigos de acceso temporales de un solo uso.

2. Proteger las operaciones de alto riesgo y valor

Los empleados que gestionan diariamente operaciones de alto riesgo y valor suelen estar en el punto de mira de los ciberdelincuentes. Una MFA robusta y moderna, como la YubiKey, permite reforzar los sistemas de alto riesgo, y garantiza únicamente el acceso autorizado a las cuentas y las transacciones autorizadas de alto valor.

3. Proteger a los usuarios con privilegios

Los usuarios con privilegios son los principales objetivos de los ciberdelincuentes, ya que tienen un mayor acceso a la información confidencial de las empresas y los clientes. Para reforzar el acceso de los usuarios con privilegios y detener los ataques dirigidos, las empresas de servicios financieros deben garantizar que se cumplan las prácticas recomendadas de seguridad en materia de autenticación, exigiendo a los usuarios con privilegios que se autentiquen con llaves de seguridad de hardware resistentes al phishing, como la YubiKey.

4. Proteger a los trabajadores de los centros de llamadas

Debido a sus características, como la elevada rotación de empleados y los cambios estacionales en el volumen de trabajo, los centros de llamadas necesitan un método seguro y sencillo para verificar la identidad de los agentes antes de proporcionarles acceso a los sistemas y datos clave. Las YubiKeys ofrecen un alto nivel de protección que permite verificar de forma segura la identidad de los agentes de los centros de llamadas antes de darles acceso a información personal y a otros datos confidenciales, o de realizar cualquier cambio en la cuenta de un cliente, como aumentar un límite de crédito. Además, a diferencia de los teléfonos móviles, con los que se pueden fotografiar datos financieros y de los clientes, las YubiKeys proporcionan una solución de autenticación segura y verificada.

5. Proteger las estaciones de trabajo compartidas

En los bancos y los centros de llamadas es habitual que los empleados compartan dispositivos y estaciones de trabajo. Los cajeros cambian de una estación a otra y los supervisores se desplazan para autorizar las operaciones. Por lo general, estos entornos se caracterizan por su mayor volumen de rotación y por emplear a trabajadores a tiempo parcial, que pueden sentir poca vinculación con la empresa. En consecuencia, existe el riesgo de que se produzcan amenazas internas. La YubiKey garantiza una autenticación segura a través de terminales de acceso compartido, estaciones de trabajo y dispositivos compartidos para evitar el acceso no autorizado a sistemas y recursos de gran valor.

6. Proteger a los clientes con un elevado patrimonio

En comparación con los nombres de usuario, las contraseñas, los códigos enviados por SMS y los códigos OTP, las YubiKeys ofrecen la mayor seguridad para proteger a los clientes y a las cuentas bancarias online de clientes con un alto poder adquisitivo frente a la apropiación de cuentas. Proporcionar a los clientes una autenticación segura y fácil de usar puede ayudar a las empresas de servicios financieros a fomentar la captación de nuevos clientes y la fidelización. Integrar la compatibilidad con las YubiKeys en la banca en línea y móvil es sencillo. Algunas empresas de servicios financieros como Vanguard, Morgan Stanley y KeyBank ofrecen a sus clientes soluciones seguras de autenticación compatibles con las llaves de seguridad de hardware FIDO.

Adquiera y distribuya fácilmente soluciones de autenticación con YubiKey a escala

Yubico ofrece planes empresariales flexibles y rentables que ayudan a las empresas con 500 usuarios o más a abandonar la MFA tradicional y desfasada, y a evolucionar a la autenticación resistente al phishing a escala.

Con la suscripción a YubiEnterprise, las empresas pueden beneficiarse de un modelo OPEX predecible, la flexibilidad para satisfacer las preferencias de los usuarios con la elección de cualquier YubiKey, actualizaciones a las YubiKeys más recientes e implementaciones más rápidas con fácil acceso a los servicios de implementación, asistencia prioritaria y un gestor de éxito del cliente específico.

Líder en autenticación de confianza

Yubico es el principal desarrollador de los estándares de autenticación WebAuthn/FIDO2 y U2F adoptados por FIDO Alliance y es la primera empresa en producir la llave de seguridad U2F y un autenticador FIDO2 multiprotocolo.

Las YubiKeys se producen en los Estados Unidos y Suecia, manteniendo la seguridad y el control de calidad de todo el proceso de fabricación.

Serie YubiKey 5

De izquierda a derecha: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano y YubiKey 5C Nano

Contacto
yubi.co/contacto

Leer más
yubi.co/finance

[1] IBM Cost of a Data Breach Report 2023

[2] Forrester, The Total Economic Impact of Yubico YubiKeys