yubico

Autenticación multi-factor antiphishing para sus empleados híbridos y remotos

Cinco pasos para mejorar la seguridad y la productividad

El trabajo híbrido y el teletrabajo han llegado para quedarse. Sin embargo, adaptarse a la naturaleza flexible del trabajo híbrido y del teletrabajo puede crear retos de seguridad informática, lo cual acelera la necesidad de ser ágiles y emprender la transformación digital. Con empleados dispersos geográficamente, la seguridad perimetral convencional y las formas de autenticación tradicionales (como nombres de usuario y contraseñas o autenticadores para móviles) ya no son adecuadas para proteger el acceso a redes, aplicaciones y datos. Los nombres de usuario y las contraseñas se pueden vulnerar fácilmente, y los autenticadores para móviles están expuestos a phishing, programas maliciosos, suplantaciones de SIM y ataques de intermediarios (MITM) que ponen a su organización en riesgo.

Proteja a sus empleados híbridos y remotos contra las ciberamenazas modernas con la YubiKey, una llave de seguridad con hardware multiprotocolo de Yubico que proporciona autenticación antiphishing de dos factores (2FA), multifactor (MFA) y sin contraseña. La YubiKey está disponible en varios formatos y proporciona una experiencia de usuario portátil y sencilla en ordenadores de escritorio, portátiles, dispositivos móviles y tabletas. La YubiKey también permite autorrestablecer las contraseñas, lo que reduce considerablemente los costes de asistencia informática. Organizaciones de todo el mundo están implementando YubiKeys para sus empleados para garantizar un acceso seguro a redes empresariales, datos o aplicaciones, y para reducir los costes operativos.

Siga los siguientes cinco pasos para proteger a sus empleados, su red y sus dispositivos con la YubiKey:

1 Habilite el acceso mediante MFA para sistemas de gestión de identidades y accesos (IAM) y proveedores de identidad

Los mejores entornos de nube e híbridos aprovechan las soluciones de IAM para que los empleados puedan trabajar sin la molestia de tener múltiples nombres de usuario y contraseñas para diferentes aplicaciones y servicios corporativos. Habilitar la autenticación multifactor en su plataforma IAM mejorará su seguridad.

Fortalezca la seguridad en toda su organización activando la autenticación multifactor con la YubiKey. Las mejores plataformas IAM como Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, OneLogin, Ping Identity y RSA SecurID® Suite son compatibles con las YubiKeys, y pueden usarse como inicio de sesión único (SSO) para aplicaciones de mensajería y videoconferencias como Microsoft Teams, Google Hangouts y Zoom.

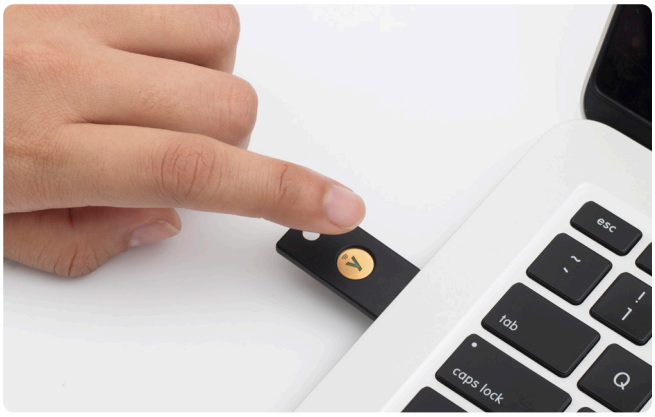
2 Elimine la dependencia de la autenticación mediante móvil para protegerse de robos de cuentas

Los métodos de autenticación en dos pasos como los códigos de un solo uso y los avisos en dispositivos dependen de dispositivos móviles expuestos a programas maliciosos, suplantaciones de SIM y ataques de intermediario. Una investigación de Google, NYU y UCSD basada en 350 000 casos reales de intentos de apropiación ha demostrado que los autenticadores mediante SMS y móvil no son muy eficaces en la prevención frente a robos de cuentas y ataques dirigidos.[1]

Integraciones de YubiKey que ayudan a proteger a sus empleados híbridos y remotos

DUO · FORGEROCK · idaptive · intercede · Microsoft · okta · ONE IDENTITY · onelogin · Onion ID · PingIdentity · secure W2

[1] Google Security Blog: New research: How effective is basic account hygiene at preventing hijacking



Proteja a sus empleados frente a robos de cuentas reemplazando los autenticadores tradicionales para móviles por la YubiKey. Haciendo uso de los modernos estándares de autenticación abierta FIDO2 y WebAuthn puede garantizar el máximo nivel de seguridad para sus trabajadores contra el phishing y los ataques de intermediarios.

3 Asegure las tecnologías de acceso remoto con autenticación multifactor

Las redes privadas virtuales (VPN) o los servidores proxy con reconocimiento de identidades (IAP) se usan en muchas organizaciones para acceder a redes corporativas, recursos protegidos o aplicaciones específicas. Conectarse a través de VPN o IAP proporciona seguridad una vez que se han establecido las conexiones, pero conectarse desde un sistema wifi inseguro de casa o público puede seguir siendo peligroso si las VPN o los IAP están protegidos con formas de autenticación tradicionales.

La YubiKey asegura el acceso remoto habilitando la autenticación de dos factores o multifactor antiphishing para las principales aplicaciones VPN como, por ejemplo, Pulse Secure y Cisco AnyConnect, así como otras aplicaciones de acceso remoto, usando tarjeta inteligente (PIV), contraseña de un solo uso (OTP), FIDO U2F o FIDO2.

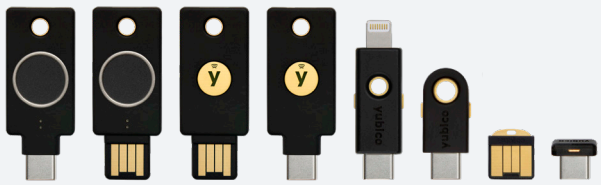
4 Proteja el inicio de sesión del ordenador con autenticación multifactor

Si los ordenadores portátiles de los empleados no están bien protegidos, pueden convertirse en puntos de entrada para amenazas externas que conlleven una violación de seguridad, lo cual puede tener repercusiones económicas, legales y de reputación para su empresa. Las YubiKeys protegen los inicios de sesión del ordenador, protegiendo las aplicaciones del dispositivo y los datos importantes de la empresa. Las múltiples opciones de inicio de sesión incluyen la autenticación para ordenadores Mac y Windows, incluyendo los que están conectados mediante Azure Active Directory, Active Directory y Microsoft Accounts. Una de las formas más eficaces de proteger el acceso al ordenador es aprovechar la funcionalidad de la tarjeta inteligente YubiKey, que requiere una YubiKey y un PIN.

5 Habilite la autenticación por pasos para los gestores de contraseñas

Muchos empleados confían en los gestores de contraseñas, pero si tu gestor de contraseñas no está protegido con MFA resistente al phishing, es vulnerable a los ataques, ofreciendo a los atacantes un repositorio de contraseñas para todas las aplicaciones y datos de tu empresa.

La YubiKey se integra con diversos gestores de contraseñas de nivel empresarial, incluyendo 1Password, Dashlane, Keeper Security y LastPass, entre otros, para garantizar que las políticas de gestión de contraseñas poco rigurosas no provoquen una violación de seguridad.



Empiece a distribuir hoy mismo YubiKeys a sus empleados híbridos y remotos

Yubico ofrece planes empresariales flexibles y rentables que ayudan a las organizaciones con 500 usuarios o más a alejarse de la MFA legacy y defectuosa y acelerar hacia la autenticación resistente al phishing a escala.

Con la suscripción YubiEnterprise, las organizaciones pueden beneficiarse de un modelo OPEX predecible, la flexibilidad para satisfacer las preferencias de los usuarios con la elección de cualquier YubiKey, actualizaciones a los últimos modelos de la YubiKey y despliegues más rápidos con fácil acceso a los servicios de despliegue, soporte prioritario y Customer success manager dedicado. Los clientes con suscripción también pueden adquirir servicios y productos adicionales.

Contacte con el equipo de ventas de Yubico hoy mismo.

Se han implementado YubiKeys en:

- **9 de las 10 principales** empresas tecnológicas mundiales
- **4 de los 10 principales** bancos de Estados Unido
- **5 de los 10 principales** minoristas mundiales

Sobre Yubico Yubico permite un inicio de sesión seguro y fácil. Como líder global en acceso seguro a ordenadores, dispositivos móviles y más, Yubico es creador y uno de los principales contribuyentes a los estándares de autenticación FIDO2, WebAuth y FIDO Universal 2nd Factor (U2F) y sistemas de autenticación abierta. Para más información, visite: www.yubico.com.

Yubico AB
Kungsgatan 44
2.ª planta
SE-111 35 Estocolmo
Suecia

Yubico Inc.
5201 Great American Pkwy
Suite 122
Santa Clara, CA 95054
EE. UU.