SEA CIBERNÉTICAMENTE INTELIGENTE
#CyberMonth

MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021: PONGA DE SU PARTE. #BECYBERSMART

AUTENTICACIÓN POR MÚLTIPLES FACTORES

¿Ha notado la frecuencia con que las violaciones de seguridad, los datos robados y el robo de identidad son regularmente las noticias de primera página hoy en día? Quizá usted, o alguien que conoce, ha sido víctima de delincuentes cibernéticos que robaron sus datos personales, credenciales bancarias o más. A medida que estos incidentes se vuelven más prevalentes, usted debe considerar el uso de la autenticación por múltiples factores, también conocida como la autenticación fuerte, o autenticación por dos factores. Es posible que ya esté familiarizado con esta tecnología, ya que muchos bancos e instituciones financieras exigen una contraseña y también alguno de los siguientes para iniciar sesión: una llamada, un correo electrónico o un mensaje de texto con un código. Al aplicar estos principios de la verificación a más de sus cuentas personales, tales como su correo electrónico, redes sociales y más, usted puede asegurar de mejor manera su información e identidad en Internet.

QUÉ ES

La autenticación por múltiples factores (MFA, por sus siglas en inglés) se define como un proceso de seguridad que exige más de un solo método de autenticación de fuentes independientes para verificar la identidad del usuario. En otras palabras, una persona que desea usar el sistema recibirá acceso solamente después de haber proporcionado dos datos que identifican únicamente a esa persona.

CÓMO FUNCIONA

Hay tres categorías de credenciales: algo que usted conoce, tiene o es. A continuación, se proveen algunos ejemplos por cada categoría.

ALGO QUE CONOCE
- Contraseña/frase de contraseña
- Número PIN

ALGO QUE TIENE
- Token o aplicación de seguridad
- Mensaje de texto, llamada o correo electrónico de verificación
- Tarjeta inteligente

ALGO QUE USTED ES
- Huella
- Reconocimiento facial
- Reconocimiento de voz

Para obtener acceso, sus credenciales deben provenir de al menos dos categorías diferentes. Uno de los métodos más comunes es iniciar sesión con su usuario y contraseña. Después, se generará y se enviará un único código a su teléfono o correo electrónico, lo cual usted ingresaría dentro del tiempo permitido. Este código único es el segundo factor.

CUÁNDO SE DEBE USAR

Se debe usar MFA para añadir otra capa de seguridad adicional en los sitios que tienen información confidencial, o cuando se desea tener una seguridad aumentada. MFA hace que sea más difícil para las personas no autorizadas iniciar sesión como el titular de la cuenta. Según el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), se debe usar MFA siempre que sea posible, en especial cuando se trata de sus datos más delicados—por ejemplo, su correo electrónico principal, sus cuentas financieras y sus registros médicos. Algunas organizaciones exigirán que use MFA; con otras, MFA es opcional. Si tiene la opción de habilitarla, debe tomar la iniciativa y hacerlo para proteger sus datos y su identidad.

ACTIVE MFA EN SUS CUENTAS INMEDIATAMENTE

Para aprender cómo activar MFA en sus cuentas, diríjase a la página de Proteja su usuario, donde encontrará instrucciones para aplicar esta forma de seguridad más fuerte en muchas páginas web y productos de software comunes que usted podría usar. Si alguna de sus cuentas no aparece en esa página de recurso, explore las configuraciones de su cuenta o el perfil del usuario para verificar si MFA está disponible como opción. Si la encuentra, ¡piense en implementarla de inmediato! Los usuarios y las contraseñas ya no son suficientes para proteger las cuentas con información confidencial. Al usar la autenticación por múltiples factores, usted puede proteger estas cuentas y reducir el riesgo de fraude y robo de identidad por Internet. ¡También debe pensar en activar esta función en sus cuentas en las redes sociales!

COMUNÍQUESE CON EL EQUIPO DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE CISA

Muchas gracias por su apoyo y compromiso continuos con el Mes de Concientización sobre Seguridad Cibernética y por ayudar a todos los estadounidenses a mantenerse seguros en Internet. Para aprender más, envíe un mensaje por correo electrónico a nuestro equipo en CyberAwareness@cisa.dhs.gov, o visite www.cisa.gov/cybersecurity-awareness-month o staysafeonline.org/cybersecurity-awareness-month/.