SEA CIBERNÉTICAMENTE INTELIGENTE

#CyberMonth

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

CÓMO CREAR UNA CONTRASEÑA

Crear una contraseña fuerte es un paso crítico que debe seguir para protegerse en Internet. El uso de contraseñas largas y complejas es una de las maneras más fáciles de defenderse de la delincuencia cibernética. Nadie es inmune al riesgo cibernético, pero #BeCyberSmart y podrá minimizar las probabilidades de un incidente.

CONSEJOS SENCILLOS

- **Use una frase de contraseña larga** Según la guía del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), usted debe pensar en usar la contraseña o frase de contraseña más larga que se permite. Por ejemplo, puede usar una frase de contraseña tal como un titular del diario o incluso el título del último libro que ha leído. También debe añadir algunos signos de puntuación y letras mayúsculas.
- **No debe ser fácil adivinar sus contraseñas** No incluya su información personal en su contraseña, por ejemplo, su nombre o el nombre de sus mascotas. Esta información suele ser fácil de encontrar en las redes sociales, y hará que sea más fácil para los delincuentes cibernéticos hackear sus cuentas.
- **Evite el uso de palabras comunes.** Sustituya letras por números y signos de puntuación. Por ejemplo, @ puede remplazar la letra "A" y un signo de exclamación (!) puede remplazar las letras "I" o "L".
- **Sea creativo.** Utilice remplazos fonéticos, tales como "PH" por la "F". O emplee errores ortográficos intencionales, pero obvios, tales como "enjin" por "engine".
- **Sus contraseñas deben mantenerse confidenciales.** No diga a nadie sus contraseñas y esté atento para los atacantes que intentan engañar a usted para hacer que divulgue sus contraseñas por correo electrónico o teléfono. Cada vez que comparte o vuelve a usar una contraseña, se disminuye su seguridad por crear otras formas adicionales en que podría ser robado o usado indebidamente.
- **Cuenta única, contraseña única.** Tener contraseñas distintas para varias cuentas ayuda a evitar que los delincuentes cibernéticos obtengan acceso a estas cuentas y proteger a usted en caso de una filtración de datos. Es importante hacer cosas diferentes—busque maneras que sean fáciles de recordar para personalizar su contraseña estándar para sitios diferentes.
- **Duplique la protección de sus credenciales.** Utilice la autenticación por múltiples factores (MFA, por sus siglas en inglés) para asegurar que la única persona con acceso a sus cuentas sea usted mismo. Úsela para su correo electrónico, su banco, sus redes sociales y todo otro servicio que requiere que inicie sesión. Habilite MFA con un dispositivo móvil fiable, tal como su teléfono inteligente, una aplicación de autenticación o un token seguro—un dispositivo físico pequeño que puede llevar en su llavero. Para más información, lea la Guía a la Autenticación por Múltiples Factores.
- **Utilice un administrador de contraseñas para recordar sus contraseñas.** La manera más segura de guardar todas sus contraseñas únicas es mediante el uso de un administrador de contraseñas. Con una sola contraseña, una computadora puede crear y guardar contraseñas para cada cuenta que usted tenga y así proteger su información en Internet, la cual incluye los números de sus tarjetas de crédito y sus códigos de tres dígitos, las respuestas a preguntas de seguridad y más.

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/.