4 consejos para crear contraseñas más fuertes y seguras

No es sorpresa que a los actores maliciosos les encanta encontrar vulnerabilidades fáciles de explotar y las contraseñas débiles están sin dudarlo en el top de la lista.

Una vez que los atacantes han logrado acceder a la cuenta de un usuario a través de una contraseña robada, salen con un tesoro de datos personales como detalles de cuentas bancarias u otro tipo de información personal crítica. Con estos datos, los atacantes pueden ejecutar un gran número de actividades maliciosas como robar la identidad del individuo, acceder a sus cuentas de redes sociales e incluso hacer cargos a sus tarjetas de crédito. Como resultado, resulta crucial que las contraseñas que se utilizan además de ser fuertes y seguras sean constantemente cambiadas para evitar que los atacantes ganen acceso.

¿Cómo acceden a nuestras contraseñas?

Existen numerosas tácticas que los atacantes utilizan para robar las contraseñas. Un ejemplo de ello es la ingeniería social- o phishing- en la cual los cibercriminales engañan al usuario para proveer credenciales a través de un correo o mensajes de texto, haciendo clic en enlaces maliciosos o visitando sitios web infectados. Otra es la intercepción de tráfico, en donde los atacantes utilizan software espía para monitorear el tráfico de la red que contiene información de contraseñas y capturan así las credenciales.

Los ciber criminales están en búsqueda constante de nuevas formas de comprometer las credenciales de los usuarios, haciendo que sea casi imposible crear una lista completa de cómo pueden robar una contraseña. Es por eso que necesitamos aprender a mantenernos a nosotros y nuestros datos seguros en línea. Un buen lugar para empezar es implementando contraseñas que sean difíciles de robar en todas nuestras cuentas.

Mejores prácticas, mejores contraseñas.

¿Qué constituye una contraseña fuerte? A continuación, cuatro consejos sencillos para crear excelentes contraseñas y protegernos así de un ciberataque.

1. **Crea contraseñas que sean imposibles de olvidar, pero difíciles para otros de adivinar.** Mientras puede parecer una buena idea añadir números o caracteres especiales a palabras comunes o frases para fortalecer tu contraseña, los atacantes pueden utilizar muchas técnicas para romper este código. Para que sea más fácil crear contraseñas fuertes puedes utilizar una regla mnemotécnica, como por ejemplo la segunda letra de cada palabra en una oración que conoces o de la letra de una canción y un mix de letras mayúsculas y caracteres especiales.
2. **Evita utilizar nombres específicos, números o frases en tus contraseñas**. Mantén tu información personal, junto con tu destino favorito de vacaciones, universidad o equipo de deportes, fuera de tus contraseñas. Evita utilizar:

- Fechas de cumpleaños
- Números de teléfono
- Información de tu compañía
- Nombres, incluyendo títulos de películas o equipos deportivos
- Una ofuscación simple de una palabra común (“P@$$w0rd”)

3. **Utiliza diferentes contraseñas para cada cuenta.** Cuando utilizas la misma contraseña para múltiples cuentas, aumentas la cantidad de información a la que un atacante puede acceder si roba tus credenciales. Los cibercriminales, que saben que es muy común que las contraseñas sean reutilizadas, van a empezar a utilizar esa información en otras cuentas hasta que logren desbloquear las que tienen la misma combinación.

4. **Usa un administrador de contraseñas para generar claves complejas y que sean fáciles de cambiar para todas tus cuentas.** Si bien, seguir los consejos anteriores es un buen lugar para empezar, es importante no utilizar un documento en tus dispositivos para anotar todas tus contraseñas (o un papel pegado a tu teclado). En su lugar, considera mejor utilizar un administrador de contraseñas como una opción más segura ya que puede generar contraseñas únicas para cada una de tus cuentas, encriptar esas contraseñas y almacenarlas en una bóveda local o basada en la nube.

Estar consciente de los riesgos de ciberseguridad y las tácticas de los atacantes es ahora más importante que nunca tanto en el trabajo como en nuestra casa. Utilizar contraseñas fuertes y seguras, y cambiarlas de manera regular, es una parte fundamental de proteger la información personal y los activos digitales.