Hoja de “Algunas Estrategias para las Contraseñas”

Introducción

Antes de comenzar la actividad, haz las siguientes preguntas a tu compañero/a:

- ¿Usas la misma contraseña para más de una cosa?
- ¿Tu contraseña incluye un número que sería fácil de adivinar, como tu cumpleaños?
- ¿Tu contraseña incluye tu nombre?

Recomendaciones básicas

- Incluye al menos un símbolo.
- Incluye al menos una letra en MAYÚSCULA y una en minúscula.
- Las contraseñas deberían tener como mínimo 7 caracteres.
- Las contraseñas deberían ser fáciles de recordar, a menos que uses un gestor de contraseñas. Un gestor de contraseñas es un sitio en la web o una aplicación que ayuda a los usuarios a guardar y organizar sus contraseñas.
- Las contraseñas no deberían ser una palabra única común ni información personal (fecha de nacimiento, nombre del padre, etc.)
- Las contraseñas no deberían compartirse en varios sitios en la web.

Indicaciones

Practica usar estos métodos pare crear nuevas contraseñas más seguras.

1. El método de la oración

En 2008, el experto en seguridad Bruce Schneier presentó un método para crear contraseñas que sigue recomendando aún hoy. Funciona así: escoge una oración y conviértela en una contraseña.

La oración puede ser cualquier cosa personal que puedas recordar. Toma las palabras de la oración, luego abrévialas y combínalas de maneras únicas para formar una contraseña. Estos son cuatro ejemplos de oraciones:

- WOO!TPwontSB = Woohoo! The Packers won the Super Bowl! (¡Los Packers ganaron el Super Tazón!)
- 1tubuupshhh…imj = I tuck button-up shirts into my jeans. (Me meto las camisas dentro de los jeans).
- W?ow?imp::ohth3r = Where oh where is my pear? Oh, there. (¿Dónde está mi pera? Ah, está allí).

Practica crear tu propia contraseña a partir de una oración:

_____

2. El método de las 12 palabras al azar

¿Sabías que ahora las contraseñas pueden ser frases? Puedes empezar con una frase como "Incluso en invierno, los perros parrandean con las escobas y los Kit Kats del vecino". Solo asegúrate de que no sea una frase sencilla o tomada de algún libro. También puedes escoger 12 palabras al azar del diccionario: "Despensa pato algodón gorra tejido aeroplano ronquido remo Navidad charco tronco carisma".

Cuando se introduce en un verificador de contraseñas, la frase de 12 palabras produce que tomarán 238,378,158,171,207 cuadragintillones de años para que un ataque directo la decodifique.

Trata de crear tu propia contraseña de 12 palabras:

_____

_____

3. El método PAO

Las técnicas de memorización y los dispositivos mnemotécnicos pueden ayudarte a recordar las contraseñas más largas. Al menos, esa es la teoría de los científicos informáticos de la Universidad Carnegie Mellon, que sugieren usar el método Persona-Acción-Objeto (PAO) para crear y almacenar contraseñas inquebrantables.

El método PAO se hizo popular en el libro de superventas de Joshua Foer, *Moonwalking with Einstein*. El método funciona así: escoge una imagen de un lugar interesante (el Monte Rushmore). Escoge una foto de un familiar o una persona famosa (Beyoncé). Imagina una acción azarosa junto con un objeto azaroso (Beyoncé conduce un molde gigante de gelatina en el Monte Rushmore).

Una vez que hayas creado y memorizado varias historias de PAO, puedes usarlas para generar contraseñas. Por ejemplo, puedes tomar las tres primeras letras de cada palabra para crear "BeyConMolGigGelMonRus".

Ahora tienes una contraseña de 21 caracteres que parecerá completamente azarosa a los demás, pero no a ti.

Crea tus propias contraseñas con el método PAO:

_____

_____