Contraseñas Seguras

UNA GUÍA RÁPIDA PARA PADRES Y ADOLESCENTES

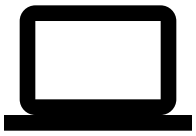
ConnectSafely

No comparta contraseñas.

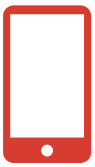
Nunca le de su contraseña a nadie. Ni siquiera a sus amigos, incluso si son muy buenos amigos. Un amigo puede , incluso accidentalmente, pasar su contraseña a otros o incluso convertirse en un examigo y abusar de ella. Una posible excepción es que los niños pequeños compartan contraseñas con sus padres.

Combínelas.

No utilice la misma contraseña en varios sitios web o aplicaciones. Si alguno de sus sitios web es hackeado o si una persona que trabaja con páginas web roba su contraseña, los criminales podrían intentar usarla en sus otros sitios web y aplicaciones.



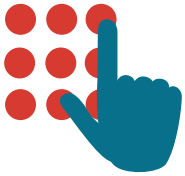
Entre más larga, mejor.



Cree contraseñas de al menos 12 caracteres de longitud. Los expertos en seguridad ahora recomiendan una "frase de contraseña" en lugar de simplemente una contraseña. Dicha frase debería ser relativamente larga, de más o menos 20 caracteres, y consistir en palabras aparentemente aleatorias unidas junto con números, símbolos y letras mayúsculas y minúsculas. Piense en algo que pueda recordar pero que los demás no puedan adivinar, como ChocolateAmarillo#56CadillacPe$cado. Evite usar citas famosas que puedan ser fáciles de adivinar.

Diversifique los caracteres.

Incluya números, mayúsculas y símbolos. Considere usar un signo $ en lugar de una S o el 1 en lugar de &, o incluir un & o %, pero tenga en cuenta que $1gno NO es una buena contraseña. Los ladrones de contraseñas están familiarizados con esta información. Pero Ma$Jeua1 (abreviatura para "Mi amigo Sam Jones es un amigo increíble") es una contraseña excelente.



*Para conocer más sobre contraseñas, visite ConnectSafely.org/passwords. Para descargar un PDF imprimible, visite Connectsafely.org/quickguides.

No las publique a simple vista.

Puede parecer obvio, pero los estudios han encontrado que muchas personas ponen una nota adhesiva con su contraseña en el monitor de pantalla. Mala idea. Si debe escribirla, oculte la nota en algún lugar donde nadie pueda encontrarla.

Considere un administrador de contraseñas.

Los programas, aplicaciones, y servicios web como RoboForm o Lastpass le permiten crear una contraseña diferente y muy segura para cada uno de sus sitios web. Solo debe recordar la contraseña para acceder al programa o asegurar la página o aplicación que almacena las contraseñas para usted.

Autenticación multifactor.

Muchos servicios ofrecen una opción para verificar su identidad en caso de que alguien inicie sesión en su cuenta desde un dispositivo no reconocido. El método más común es enviar un texto u otro tipo de mensaje a un dispositivo móvil registrado con el código que debe digitar para verificar que realmente es usted. En la mayoría de los casos, no será necesario utilizar este código cuando inicie sesión desde un dispositivo conocido como su propia computadora, tableta o teléfono.

No caiga en fraudes electrónicos.

Sea muy cuidadoso antes de hacer clic en un enlace (incluso si parece ser de un sitio legítimo) que le pida iniciar sesión, cambiar su contraseña o proporcionar cualquier otra información personal. Puede que sea legítimo o puede ser un fraude electrónico donde la información que ingrese va a un hacker. En caso de duda, inicie sesión manualmente digitando la URL que sabe que pertenece a la página web en la ventana de su navegador.

Asegure sus sistemas.

Es posible que la mejor contraseña del mundo no le sirva de nada si alguien está mirando por encima de su hombro mientras la digita o si olvida cerrar sesión en una computadora de un cibercafé. El software malintencionado, incluyendo los "capturadores de teclado" que registran todas las pulsaciones, se han utilizado para robar contraseñas y otra información. Para aumentar la seguridad, asegúrese de estar usando un software antimalware actualizado y que su sistema operativo esté actualizado.

Proteja su teléfono.

La mayoría de los teléfonos se pueden bloquear de modo que la única forma de usarlos es digitando un código. Generalmente se trata de una cadena de números o tal vez un patrón que debe dibujar en la pantalla. Algunos teléfonos nuevos le permiten registrar huellas digitales, que son bastante seguras. En ocasiones, cuando las personas con malas intenciones se encuentran teléfonos desbloqueados, los utilizan para robar la información de los propietarios, hacer llamadas o enviar mensajes de texto que parecen provenir del dueño. Alguien, haciéndose pasar por usted, podría enviar mensajes de texto que parezcan que está intimidando o acosando a alguien en su libreta de contactos con imágenes o palabras inapropiadas. Aprenda cómo utilizar servicios como iCloud o Encontrar mi dispositivo de Google para poder localizar, bloquear o eliminar la información de su teléfono en caso de pérdida o robo.

52%

De los adultos en línea han usado la autenticación de dos factores en sus cuentas en línea.

*Pew Research Center

57%

De los usuarios en línea dicen que varían sus contraseñas en sus cuentas en línea.

*Pew Research Center

39%

De los usuarios en línea dicen que la mayoría de sus contraseñas son las mismas o muy similares entre sí.

*Pew Research Center