Título:	Consejos para Mantenerse Seguro en Línea: Video sobre Cómo Crear y Gestionar Contraseñas.
Presentación:	La Serie de Videos Consejos para Mantenerse Seguro en Línea se organiza mediante diapositivas como marcadores visuales. Cualquier imagen de las diapositivas que sea importante para el contenido, y exprese cualquier información adicional más allá del guion, se incluye aquí como texto alternativo.
Narrador:	Bienvenidos al video de Help@Hand Consejos para Mantenerse Seguro en Línea: Parte 2: Video sobre Cómo Crear y Gestionar Contraseñas. Help@Hand es una Colaboración de múltiples ciudades y condados creada para ayudar a dar forma al futuro de soluciones de salud mental basadas en la tecnología y conectar a las personas con los cuidados por todo el estado. La intención de estos tutoriales en video es empoderar a las comunidades de California para que tomen decisiones informadas sobre la forma en que interactúan con la tecnología.
Narrador:	Este es el Curso 3 de una serie de 4 cursos llamada Consejos para Mantenerse Seguro en Línea Parte 2. Los videos de esta serie pueden verse por orden, o en cualquier orden según sus intereses. En este video presentaremos estrategias para crear y gestionar contraseñas en línea. Los consejos que siguen pueden ayudarle a crear contraseñas fuertes que sean difíciles de descubrir, lo cual puede reducir el riesgo de que extraños accedan a sus datos personales.
Imagen:	Se muestra un ejemplo de contraseña con 10 caracteres. La contraseña es una f minúscula, P mayúscula, libra, asterisco, L mayúscula, v minúscula, el signo &, 2, por ciento, a minúscula.
Narrador:	El primer paso es hacer que su contraseña sea larga. En general, su objetivo debe ser incluir 10 caracteres. Una contraseña corta que solo tenga 4-5 caracteres es mucho más fácil de adivinar que una que tiene 10 caracteres o más, como la que se muestra.
Imagen:	Se muestra un ejemplo de contraseña con 10 caracteres. La contraseña es una f minúscula, P mayúscula, libra, asterisco, L mayúscula, v minúscula, el signo &,2, por ciento, a minúscula. Esta imagen se mueve para destacar las letras en mayúscula (P y L) y las letras en minúscula (f,v,a).
Narrador:	Cuando esté creando su contraseña, debe usar letras tanto mayúsculas como minúsculas. Como puede ver aquí, no solo la contraseña tiene 10 caracteres, sino que además contiene mayúsculas y minúsculas.
Imagen:	Se muestra un ejemplo de contraseña con 10 caracteres. La contraseña es una f minúscula, P mayúscula, libra, asterisco, L mayúscula, v minúscula, el signo &,2, por ciento, a minúscula. Esta imagen se mueve para destacar los números 2 y los símbolos de la libra, el asterisco, el signo &, por ciento.
Narrador:	También debe incluir una variedad de números y símbolos que puede encontrar en la parte superior de su teclado. Usando de nuevo el ejemplo de esta contraseña, ´verá que contiene números y símbolos que la hacen más difícil de adivinar.
Imagen:	Se muestra en pantalla una Tarjeta del Seguro Social en la que se ve el nombre completo del titular de la tarjeta y su número del seguro social, una imagen que

muestra “Fecha de Nacimiento”, y una sección de un mapa que pretende mostrar una “Dirección”.

Narrador: A veces tenemos la tentación de utilizar fragmentos de nuestra información personal dentro de nuestras contraseñas para hacerlas más fáciles de recordar. El problema de esta estrategia es que los estafadores también puede que conozcan alguna de esta información y la utilizarán cuando intenten adivinar sus contraseñas. Por ejemplo, si un estafador conoce su nombre y dirección, puede que intente combinaciones de contraseñas que incluyan esta información. Por eso lo mejor es dejar todos los detalles personales fuera de sus contraseñas.

Imagen: Se muestran dos ejemplos distintos de contraseñas. La primera contraseña (a la izquierda) es la siguiente: B mayúscula, menos que, signo más, signo de interrogación, 3, g minúscula, 9, w minúscula, paréntesis de cierre, barra invertida. La segunda contraseña (a la derecha) es la siguiente: K mayúscula, a minúscula, t minúscula, e minúscula, 1,2,3.

Narrador: Ahora que usted ha aprendido algunos consejos para crear contraseñas fuertes, dediquemos un momento a revisar estas dos contraseñas diferentes. ¿Cuál es más segura? ¿La de la derecha o la de la izquierda?

Narrador: La contraseña de la izquierda sería más difícil de adivinar para nadie porque es larga, tiene letras mayúsculas y minúsculas, símbolos y números y no contiene ninguna información personal, lo cual la hace más segura. Sin embargo, la contraseña de la derecha sería muy fácil de adivinar porque incluye el nombre de la persona y es muy corta y sencilla, lo cual la hace menos segura.

Imagen: Se muestran tres iconos que designan diferentes plataformas en línea, desde una cuenta de correo electrónico a una cuenta de compras en línea. También hay tres ejemplos distintos de contraseña, cada una alineada con una imagen. La primera contraseña es 4, asterisco, igual, M mayúscula, k minúscula, signo de exclamación, tilde, símbolo del dólar, p minúscula. La segunda contraseña es B mayúscula, menos que, signo más, 3, g minúscula, 9, 9 minúscula, w minúscula, paréntesis de cierre, barra invertida. La tercera contraseña es libra, símbolo del dólar, signo de exclamación, B mayúscula, j minúscula, guion, K mayúscula, 2, 6, por ciento.

Narrador: Ahora que sabe cómo crear una contraseña fuerte, es importante que utilice contraseñas distintas para cada cuenta en línea. Si usted solo usara una única contraseña para todas sus cuentas, entonces si alguien adivinara esa contraseña única, podría acceder a su banco en línea y cuentas de compras y correo, por nombrar solo unas pocas. Como ven, esta persona ha creado contraseñas diferentes para cada una de las tres cuentas, lo cual hace más difícil para un estafador acceder a su información.

Narrador: Otro consejo es cambiar sus contraseñas a menudo. Hacer esto es especialmente importante si cree que ha sido víctima de un fraude.

Narrador: Si sigue los consejos que hemos mencionado hasta ahora para crear contraseñas únicas y complicadas para cada una de sus cuentas en línea, probablemente estará preguntándose cómo poder recordarlas todas. En lugar de escribirlas en papel, puede almacenarlas de forma segura en línea con un gestor de contraseñas que almacene

sus contraseñas para sitios distintos. Hay diversos gestores de contraseñas disponibles de forma gratuita o con un costo reducido. Vea, al final de este tutorial, algunos ejemplos de gestores de contraseñas que puede que quiera probar.

Narrador: Si sigue los consejos que hemos mencionado hasta ahora para crear contraseñas únicas y complicadas para cada una de sus cuentas en línea, probablemente estará preguntándose cómo poder recordarlas todas. En lugar de escribirlas en papel, puede almacenarlas de forma segura en línea con un gestor de contraseñas que almacene sus contraseñas para sitios distintos. Hay diversos gestores de contraseñas disponibles de forma gratuita o con un costo reducido. Vea, al final de este tutorial, algunos ejemplos de gestores de contraseñas que puede que quiera probar.

Narrador: En resumen, cuando cree contraseñas, intente hacerlas lo más difíciles de adivinar que sea posible. Puede hacer esto haciéndolas largas, utilizando letras mayúsculas y minúsculas así como símbolos y números. Aunque puede ser tentador incluir información personal, esto hace más fácil para los hackers adivinar su contraseña..

Narrador: Algunas estrategias adicionales consisten en tener contraseñas diferentes para cada sitio y cambiarlas con frecuencia. Y finalmente, pruebe a usar un gestor de contraseñas para almacenar todas sus contraseñas fuertes.

Imagen: Se muestran tres gestores de contraseñas en línea distintos. La lista incluye Last Pass, 1Password y Google Chrome Password Manager.

Narrador: Aquí tiene algunos de los recursos de Gestores de Contraseñas mencionados anteriormente, para ayudarle a recordar sus contraseñas; algunos son gratuitos y otros de bajo costo.

Narrador: Esperamos que haya encontrado útil este video. A pesar de que es opcional, le rogamos que, por favor, dedique un minuto a proporcionar retroinformación sobre su experiencia, haciendo clic en el enlace de encuesta que aparecerá en breve. Gracias por participar, y no olvide ver los demás videos de Help@Hand