Privacidad en línea: contraseñas y autenticación de dos factores (2FA)

THE KANSAS CITY PUBLIC LIBRARY TECHACCESS

Término	Definición
Clave	Una combinación secreta de letras, números y símbolos que solo usted conoce, que le permite acceder a una cuenta, cambiar configuraciónes y actualizar detalles de una cuenta
Autenticación de dos factores (2FA)	Una forma de acceder a una cuenta que requiere dos formas separadas de identificación. La primera es una contraseña. El otro puede ser un código enviado a su teléfono inteligente o una pregunta de seguridad que configuro usted mismo
Nombre de usuario	Una combinación de letras, números y símbolos que lo identifican como un usuario de cuenta; si se trata de una cuenta en línea, otros pueden ver el nombre de usuario

Privacidad en línea: contraseñas

Cuando crea una cuenta, debe crear tanto un **nombre de usuario** como **una contraseña** para poder configurar la cuenta según sus especificaciones. También significa que su configuración será la misma, ya sea que acceda a su cuenta desde su teléfono o dispositivo personal como una computadora o tableta, o un dispositivo público, como la computadora de una biblioteca.

Debido a que cada cuenta que crea necesita un nombre de usuario y una contraseña, es posible que le resulte más fácil hacer que su contraseña sea la misma para todas sus cuentas en línea.

Pero esto puede ser muy peligroso y facilitar que alguien Hackeé su cuenta. Si usa la misma combinación de nombre de usuario y contraseña para varias cuentas, está comprometiendo su seguridad en línea. Si alguien descifrara su contraseña, puede intentar hackear otras cuentas utilizando la misma combinación de nombre de usuario y contraseña.

¿Qué hace que una contraseña sea segura?

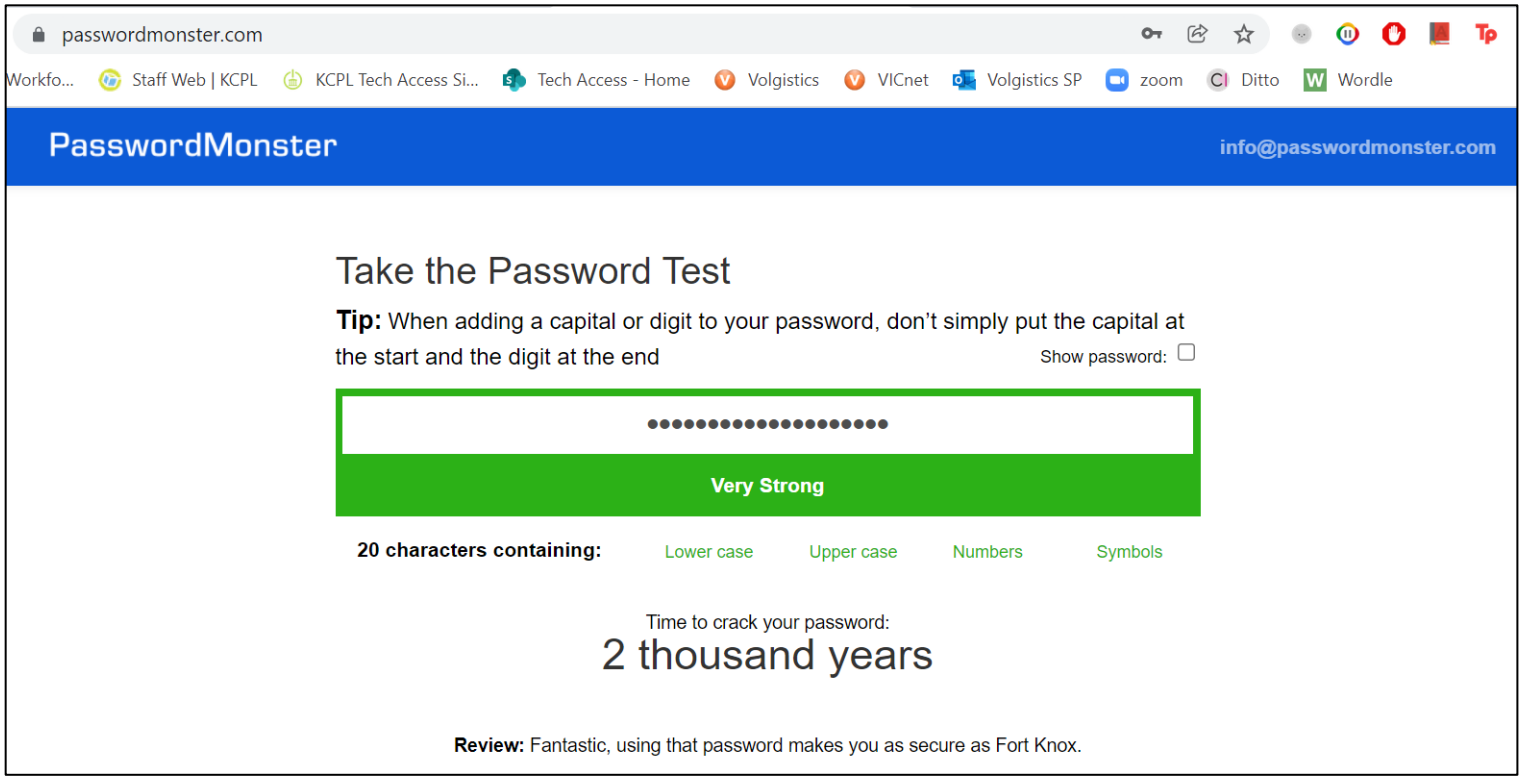
Usando la lista a continuación del **Privacy Rights Clearinghouse**, considere cómo puede usar estas características para crear sus propias contraseñas seguras para proteger su privacidad en línea.

- Evite el uso de palabras del diccionario.
  - **Ejemplo:**Los Angeles, Orlando
  - **Por qué:**Fácil de descifrar para los hackers informáticos utilizando un diccionario electrónico, que puede sustituir números y símbolos por letras similares.
- No use información personal.
  - **Ejemplo:**SurCalle4, AnaMaria89
  - **Por qué:**La información personal se puede encontrar fácilmente, incluida cualquier parte de su nombre, cumpleaños, número de Seguro Social o dirección.
- Evite secuencias comunes de números o letras.
  - **Ejemplo:**qwerty, 123456, abc987789cba
  - **Por qué:**Las combinaciones secuenciales son muy fáciles de adivinar.
- Utilice símbolos cuando sea posible.
  - **Ejemplo:**t# ym31of0urF@ve $especial$
  - **Por qué:**Crea más permutaciones de posibles palabras, por lo que es más difícil de adivinar.
- Hazlo más largo.
  - **Ejemplo:**S1ngusa$ongy0uret3ep1anomaN
  - **Por qué:**Las contraseñas se vuelven más difíciles de descifrar cuanto más largas son.
- Considere usar la primera letra de cada palabra en una oración, frase, poema o título de una canción como contraseña.
  - **Ejemplo:** 0u@mdw1pw &w
  - **Por qué:**Esto crea una contraseña que parece aleatoria pero tiene un significado real que puede recordar.
- Cree diferentes contraseñas para diferentes cuentas y aplicaciones.
  - **Por qué:**Si se viola una contraseña, sus otras cuentas tampoco estarán en riesgo.

- Escriba sus contraseñas y guárdelas en un lugar seguro bajo llave.
  - **Por qué:**Si crea numerosas cuentas y no recuerda todos sus nombres de usuario y contraseñas, es importante tenerlos en algún lugar que solo usted pueda encontrar.
- Considere usar un administrador de contraseñas seguro.
  - **Por qué:**Un administrador de contraseñas en línea puede almacenar y crear contraseñas seguras para usted.
- Si ya ha establecido una contraseña que no es segura, ¡cámbiela!
  - **Por qué:**Para proteger su cuenta ahora que tiene más consejos sobre cómo crear contraseñas seguras. Busque un enlace en la página de inicio del sitio que lo dirija a la administración de cuentas y contraseñas.

En caso de duda, utilice un sitio web como https://www.passwordmonster.com/ para determinar el nivel seguridad de sus contraseñas y asegúrese de incluir todos los caracteres que componen una contraseña segura.

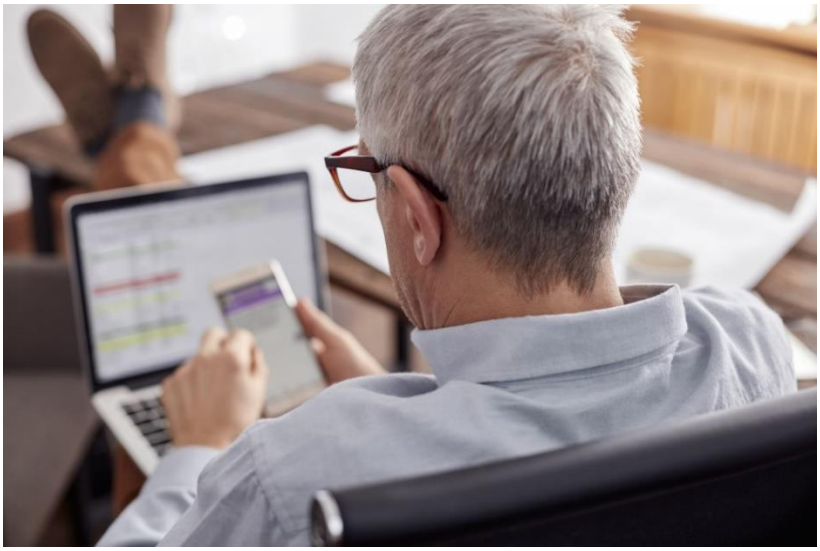
(En el ejemplo de la imagine abajp dice que tomaria 2000 años para decifrar la contraseña que probo una persona provando diferentes contraseñas usando el sitio web de Password master)



Privacidad en línea: contraseñas y autenticación de dos factores (2FA)

THE KANSAS CITY PUBLIC LIBRARY
TECH ACCESS

Privacidad en línea: autenticación de dos factores



Cuando pensamos en la seguridad y protección en línea, lo primero que nos viene a la mente son las contraseñas seguras. Pero en la última década más o menos, otro método se ha vuelto popular para proteger su información en línea: **la autenticación de dos factores (2FA)**. 2FA se trata de confirmar que eres quien dices ser cuando inicias sesión en una cuenta. La mayoría de los sitios requieren 2FA como estándar mínimo de seguridad.

Un **factor de autenticación** es una prueba que un usuario debe presentar para demostrar que es quien dice ser.

Hay tres tipos de factores:

- El factor de ***conocimiento*** es algo que sabes: una contraseña.
    - Estos son los más fáciles de piratear/hackear, porque solo hay un número limitado de combinaciones posibles de números, letras y símbolos en una contraseña.
- El factor ***posesión*** es algo que tienes, como un teléfono celular.
    - Si bien puede ser fácil descifrar la contraseña de alguien, es mucho más difícil piratear/hackear la cuenta si también tiene un código enviado a su teléfono para confirmar que realmente es usted quien intenta ingresar a su cuenta.
- El factor de ***inherencia*** es algo que representa quién eres, como una huella dactilar.
    - A menos que sea el propietario de la cuenta, es casi imposible falsificarla, lo que la convierte en la opción de seguridad más sólida de las tres.

Al combinar al menos dos de estos factores, está configurando dos capas protectoras entre usted y cualquier persona que intente piratear/hackear su cuenta por motivos maliciosos. Una combinación muy común es usar una contraseña y luego recibir una notificación en su teléfono que usted confirma, diciéndole a su cuenta que es usted quien intenta acceder a ella.

Aunque puede parecer intimidante configurar la autenticación de dos factores, está creando un sistema de seguridad más sólido para usted y protegiendo su información cuando lo hace. Con una aplicación como Authy o Google Authenticator, puede configurar fácilmente 2FA y asegurarse de proteger su información y sus cuentas lo mejor que pueda.

Privacidad en línea: contraseñas y autenticación de dos factores (2FA)

THE KANSAS CITY PUBLIC LIBRARY
TECH ACCESS

Referencias:
Creación de contraseñas seguras:https://edu.gcfglobal.org/en/internetsafety/creando-contraseñas-seguras/1/
Prueba de seguridad de la contraseña:https://www.passwordmonster.com/
10 reglas para crear una contraseña resistente a piratas informáticos:https://privacyrights.org/resources/10-rules-creating-hacker-resistent-password
Cómo configurar la autenticación de 2 factores:https://seniorplanet.org/how-to-set-up-2-factor-authentication/
Autenticación multifactor para personas mayores:https://www.gwadvisors.net/multi-factor-authentication/