BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

Creando contraseñas fuertes

Las contraseñas son la primera línea de defensa contra cibercriminales (hackers) al conducir transacciones en línea (i.e. bancarias, pagando cuentas, o haciendo compras). Si los cibercriminales ganan acceso no autorizado a su computadora, ellos pueden ver su información personal; personificarle a usted y enviar mensajes a sus amigos; cambia su contraseña y bloquea el acceso a su propia cuenta; robar su identidad; o infecta sus archivos con virus. Por lo tanto, es importante escoger contraseñas fuertes que sean diferentes para cada una de sus cuentas y actualizar sus contraseñas regularmente.

Aquí hay unos consejos que le ayudaran a proteger sus transacciones en el internet:

- **Utilice una contraseña exclusiva para cada una de sus cuentas importantes tales como correo electrónico y cuentas bancarias de internet**
  Tener la misma contraseña en cada una de sus cuentas en el internet es como usar la misma llave para su hogar, auto y oficina – si un criminal gana acceso a una, las tres están en peligro y puede conducir a robo de identidad. No utilice una misma contraseña para un boletín informativo en el internet que sea la misma para su correo electrónico o su cuenta bancaria. Puede ser menos conveniente, pero utilizando múltiple contraseñas le mantendrá más seguro.

- **Genere una contraseña fuerte al combinar números, letras y símbolos**
  Las contraseñas fuertes son fácil de recordar pero difícil de adivinar. Haga sus contraseñas fuertes para ayudarle a mantener su información segura. Añadir números, símbolos y letras mayúsculas y minúsculas mezcladas hace más difícil para los cibercriminales o a otras personas el adivinar su contraseña. No utilice contraseñas obvias tales como “123456” o “contraseña”, y evite el utilizar información públicamente disponible tal como su número de teléfono, el nombre de su mascota, un niño o alguna otra persona familiar. Asimismo, evite objetos que pueden ser investigados, tales como su fecha de nacimiento o código postal.

  Largas=Fuertes. Sus contraseñas deben de tener un mínimo de 8 caracteres, pero lo más larga que pueda hacerla, lo más difícil será para un ladrón descifrar sus códigos. Mientras que es mejor evitar usar palabras reales como parte de su contraseña, si lo hace, usted puede intentar a reemplazar caracteres por algunas de las letras, e.g. $ por la letra S, o un Zero por la letra O. Otra forma puede ser añadir una cadena de caracteres o números en medio de una letra real, así convirtiéndola en dos no-letras.

- **Trate de utilizar una frase que solo usted conoce.**
  Puede empezar con “**Mis amigos Mary y Jack me envían un texto gracioso a diario**” y entonces utilice números y letras para recrearlo en algo similar a esto: **MaM&Jmeutgad** – una contraseña con muchas variaciones que será difícil para cibercriminales descifrar. Otro ejemplo sería algo como: **Ye:)deA!** – este tiene 9 caracteres que dice “**¡Yo estoy feliz de estar aquí**! Elabore un sistema para crear sus propias

frases de contraseñas. Esto hará más fácil crear contraseñas nuevas y al mismo tiempo de ayudarle a recordarlas.

- **Añadir un número de teléfono móvil**
  Algunas veces usted puede añadir un número de teléfono a su perfil para recibir un código para reestablecer su contraseña a través de un mensaje de texto. Tener un número de teléfono móvil en su cuenta es una de las más fáciles y más confiables formas de ayudarle a mantener su cuenta segura. Por ejemplo, los proveedores de servicio pueden usar el número de teléfono para desafiar a aquellos que traten de entrar en su cuenta, y pueden enviarle un código de verificación para que usted gane acceso a su cuenta si por alguna razón pierde acceso. Su número móvil es un método más seguro de identificación comparado a su cuenta de correo electrónico o alguna pregunta de seguridad porque al compararla con las otras dos, usted tiene posesión física de su teléfono móvil.

- **Active la autenticación de dos factores si se ofrece.**
  El sistema de autenticación de dos factores es un capa adicional de protección que combina algo que usted tiene, tal como un identificador físico ya sea una tarjeta o código, con algo que solo usted sabe, tal como algo memorizado, ya sea un número de identificación personal (PIN) o una contraseña.

- **Utilice una pregunta de seguridad que sea única**
  Si usted no puede, o no desea añadir un número de teléfono a su cuenta, muchos sitios de internet pueden pedirle que seleccione una pregunta para verificar su identidad en caso de que haya olvidado su contraseña. Si el servicio que usted está usando le permite crear su propia pregunta, trate de crear una pregunta que tenga una respuesta que solo usted conoce y no es algo que usted haya publicado públicamente o compartido en medios sociales. Trate de encontrar una forma de hacer su respuesta única pero memorable – así que si alguien trata de adivinar la respuesta, ellos no sabrán como introducirla propiamente.

- **Configure sus opciones de recuperación de contraseñas y manténgalas actualizadas**
  Si usted olvida sus contraseñas o no puede accederlas, usted necesitara una forma para entrar a sus cuentas. Muchos servicios le enviarán un correo electrónico a una dirección de correo electrónico de reactivación si usted necesita restaurar su contraseña. Asegúrese de que su dirección de correo electrónica para reactivación está actualizada y es una cuenta a la cual usted tiene acceso, o permita que sea enviada por texto a su teléfono móvil.

- **Mantenga sus contraseñas en un lugar seguro y que no es visible**
  Escribir sus contraseñas no es necesariamente una mala idea, pero asegúrese de mantener estas notas en un lugar seguro. No las deje a la vista o fácilmente accesibles.

  Considere utilizar un organizador de contraseñas. Los más básicos organizadores de contraseñas actúan como una caja fuerte o bóveda en su computadora. Usted puede crear contraseñas que sean únicas, complejas y fuertes, aunque nunca necesite recordarlas para cada página de internet que necesite acceder. El organizador las recuerda y las almacena así que cuando las necesite, el organizador puede ingresar su información de acceso, incluyendo la contraseña para que usted puede accederlas en forma segura.

  Estas contraseñas se almacenan en el organizador, aseguradas por una contraseña maestra que usted necesitará recordar. Esto facilita crear contraseñas fuertes que usted no necesita memorizar. ¡Una manera más fácil de almacenar en forma segura su colección de contraseñas comparada a escribirlas en un pedazo de papel! Usted necesitará investigar la variedad de productos disponibles para ver cual tiene la combinación correcta de características que funcionarán mejor para sus necesidades.

Para más información o para presentar una queja visite nuestra página web o comuníquese con el Departamento de Protección al Consumidor.

Departamento de Protección al Consumidor
2811 Agriculture Drive
PO Box 8911
Madison, WI 53708-8911

Correo Electrónico:
DATCPHotline@wi.gov

Sitio de Internet:
Datcp.wi.gov

(800) 422-7128

Fax: (608) 224-4677

TTY: (608) 224-5058

I:\dtcp\common\Fact Sheets\IDTheftPasswordsCreatingSPANISH919 06/18