Título: Consejos para Mantenerse Seguro en Línea: Cómo Actuar después de un Fraude o Ataque de Malware

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 Cómo Actuar después de un Fraude o Ataque de Malware. 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. Este es el curso [4] de una serie de 4 cursos llamada Consejos para Mantenerse Seguro en Línea. Los videos de esta serie pueden verse por orden, o en cualquier otro orden según sus intereses.

Narrador: Incluso cuando hacemos lo posible para identificar sitios web y correos electrónicos seguros, a pesar de todo podemos aún encontrarnos que somos víctimas de fraudes en línea o ataques de malware. El siguiente video compartirá algunos consejos sobre qué hacer si esto le sucede a usted.

Narrador: Se produce un fraude por Internet cuando se engaña a alguien para que comparta sus datos personales en línea, lo cual puede incluir su información de tarjeta de crédito, nombres y contraseñas de usuarios, e información relacionada con su identidad, como su nombre, número del seguro social y fecha de nacimiento.

Narrador: Una forma en la que puede producirse un fraude por internet es mediante phishing, que son intentos de obtener información sensible como nombres de usuario, contraseñas y datos de tarjetas de crédito haciéndose pasar por una entidad confiable. Esto puede ocurrir mediante correos electrónicos, sitios web o anuncios que a primera vista parecen reales.

Narrador: También podemos descargar accidentalmente malware, programas que pueden causar daño a nuestras computadoras y dar a otras personas acceso no autorizado para hacerse con datos personales. Esto puede suceder mediante anuncios que se abren en su pantalla, sitios web falsos o enlaces y adjuntos en correos electrónicos.

Narrador: Hay un tipo de malware llamado virus, porque puede infectar su computadora para modificar la forma en que funciona, y está diseñado para extenderse a otras.

Narrador: Si está preocupado por si un estafador pueda haber accedido a sus datos personales, o si cree que puede haber descargado malware, aquí tiene cinco cosas que puede hacer para limitar los daños y protegerse en el futuro. Si es posible, es mejor seguir la totalidad de estos cinco pasos para incrementar las posibilidades de que su información se mantenga segura.

Imagen: Diapositiva de una presentación, el título dice “Consejo #1” y el cuerpo del texto dice “Cambiar Contraseñas”; hay también una imagen de una ventana emergente que permite un cambio de contraseña.

Narrador: Si cree que puede haber sido víctima de un fraude, es buena idea cambiar las contraseñas de todas sus cuentas en línea. Esto hará más difícil al autor del fraude acceder a su cuenta de correo y sitios web de operaciones bancarias en línea y de compras.

Imagen: En la parte superior de la diapositiva hay una imagen con un candado. En el cuerpo de texto dice “Contraseña Débil: Kate1/22/68” con una “X” roja al lado, y la siguiente línea de texto dice “Contraseña Fuerte: T5%9Llf$4a!” con una marca de corrección verde a su lado.

Narrador: In general, es mejor crear contraseñas que sean largas, complicadas, tengan tanto números como letras, y que no contengan ninguna información personal como su nombre, fecha de nacimiento o dirección. Como puede ver aquí, la primera contraseña no es tan segura, porque contiene el nombre y la fecha de nacimiento de la persona. La segunda contraseña es mucho más segura porque es complicada, incluye números, letras y símbolos, y no contiene ninguna información personal. Usted puede ver nuestro tutorial “Cómo crear y gestionar contraseñas fuertes” para más información sobre este tema.

Narrador: Otra cosa que debe hacer después de un fraude es notificar a las tres oficinas principales de crédito que puede que un estafador haya accedido a sus cuentas. Estos incluyen Experian, Equifax y TransUnion. También debe pedir que activen una alerta de fraude para sus cuentas.

Narrador: El tercer consejo es contactar a su banco y compañías de tarjetas de crédito para congelar sus cuentas a fin de evitar que otras personas hagan cambios no autorizados.

Imagen: La diapositiva se titula “Consejo #4” con una línea de texto que dice “Actualice el software de su computadora” y debajo de esto hay un ejemplo de una ventana emergente en una computadora Mac, que dice “Actualización de Software. Hay una actualización disponible para su Mac. Actualización macOS 10.14.1. Más información…”

Narrador: Este es el consejo 4: si tiene una computadora, pruebe a actualizar su software por si su computadora ha sido infectada por malware o un virus. Actualizar el software de su computadora significa que su computadora tendrá las protecciones más actualizadas destinadas a impedir que los virus dañen su computadora.

Narrador: Si todavía no ha descargado este tipo de programas, vea nuestro tutorial “cómo descargar programas antivirus y antimalware”

Imagen: Esta diapositiva tiene tres imágenes diferentes que van cambiando durante el diálogo. El título dice “Consejo #5” y el cuerpo del texto dice “Haga un escaneado de sistema”; la primera imagen muestra una herramienta de software antivirus y antimalware de Norton. La segunda imagen muestra una herramienta de software Antivirus de Windows. La tercera imagen es de una ventana emergente que dice “Escaneado Competo. Escanea su computadora completa. Le recomendamos que ejecute un Escaneado completo inmediatamente después de instalar la aplicación. Recuerde que esto puede tomar algo de tiempo.”. Bajo ese texto hay un botón en el que se puede hacer clic que dice “Escanear” y en la parte inferior hay una ventana

emergente adicional que dice “Escaneado Completo completado hace 1 día. 104,967 archivos escaneados. 4 objetos procesados: 4 borrados.” También hay una línea en la que se puede hacer clic que dice “Informe Detallado.”]

Narrador: Y finalmente, si tiene ya programas antivirus o antimalware instalados en su computadora, haga un escaneado completo del sistema para localizar cualquier programa sospechoso.

Narrador: Recapitulemos: cuando piense que ha sido víctima de un fraude, asegúrese de:

a. Cambiar sus contraseñas
b. Avisar a sus oficinas de crédito
c. Contactar a su banco y compañías de tarjetas de crédito
d. En resumen, cuando piense que ha sido víctima de un fraude, asegúrese de:
e. Actualizar el software de su computadora
f. Ejecutar un escaneado de sistema.

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.