CPLT pide cuidar acceso a cuentas y dispositivos en período de incremento de compras online

Además la institución llamó a las empresas a “ser leales” con sus clientes en el resguardo y uso de la gran cantidad de datos personales que reciben. En un contexto en el que la ciberseguridad y la privacidad son cada vez más relevantes y en el período navideño en el que se intensifican las compras *online*, el Consejo para la Transparencia (CPLT) hizo un llamado a los usuarios al autocuidado a través de la generación de contraseñas más seguras con el fin de reducir uno de los riesgos más críticos en materia de seguridad informática, el ***password cracking o descifrado de claves***.

Este tipo de prácticas, explicó el presidente de CPLT, Marcelo Drago, permite a “piratas informáticos” acceder a contraseñas débiles y controlar dispositivos digitales, cuentas y plataformas que les permiten acceder a datos personales de los usuarios.

El Consejo detalló que el generar claves más complejas de acceso a casillas de correos electrónicos, cuentas de usuarios de servicios web o aplicaciones móviles y dispositivos digitales, permite proteger de mejor forma recursos que posibilitan acceder a información personal valiosa y sensible (como direcciones, antecedentes financieros, imágenes, entre otros contenidos), y que pueden ser objeto de una intrusión indeseada.

Sin embargo, también destacó como uno punto relevante la responsabilidad de las empresas que son las receptoras de gran cantidad de datos, debiendo asegurar su adecuado manejo y

tratamiento bajo estándares de seguridad que deben ser claros y conocidos por sus clientes.

“El autocuidado es un aspecto muy relevante en la tarea de proteger nuestros datos personales, por eso hay que tomar precauciones para acceder a cuentas de correo, Internet, banco, entre otras muchas plataformas y servicios que piden nuestros datos. Pero, las precauciones que tomemos como usuarios no son contraproducentes sino que complementan a las acciones que deben implementar las empresas en relación al resguardo y uso de mis antecedentes”, afirmó Drago.

El presidente del CPLT aprovechó de hacer un llamado a las empresas que aumentan en esta época las ventas, tanto presenciales como en el contexto digital, a “ser leales” con los usuarios y compradores dando a conocer de forma clara las políticas de privacidad.

“Las empresas chilenas tienen que ser leales con sus clientes transparentando sus políticas de privacidad, porque los datos que uno entrega a una empresa siguen siendo míos por mucho que los haya entregado. Al recibir mi información la empresa no puede hacer cualquier cosa con ese dato y tiene que hacerse responsable de su utilización. Yo tengo derecho a mantener el control de mis cuentas y también de los datos que entrego”, sostuvo.

Drago, además comentó que en la actualidad el compartir datos es y seguirá siendo una práctica habitual, por lo que adquiere suma relevancia el control que el usuario debe mantener sobre este tipo de información.

“En la sociedad actual tenemos que compartir nuestros datos personales, es algo natural. Por ejemplo, cuando usamos una aplicación del teléfono y entregamos la localización. Pero esa empresa que consigue mi localización no tiene derecho a hacer lo que quiera y entregar o usar mis datos para otros fines sin mi autorización y consentimiento expresos”, subrayó.

Algunas recomendaciones

Dada la gran cantidad de dispositivos, cuentas y servicios digitales -tanto de uso personal como laboral- que maneja los usuarios de forma cotidiana (PIN numérico, contraseña alfanumérica o patrón de desbloqueo), se sugiere entre otras medidas: no usar una única contraseña maestra y mantenerla para todos los dispositivos y plataformas; tampoco usar números derivados de direcciones, números telefónicos, fechas de cumpleaños. Se sugiere crear contraseñas que contengan números y letras y combinar mayúsculas, minúsculas y símbolos.

Se adjunta documento con todas las recomendaciones.

Recomendaciones Contraseñas CPLT

Recomendaciones para la creación y uso de contraseñas seguras

1. **Evita usar una única contraseña maestra.** Mantener una sola clave universal para todos nuestros servicios y cuentas implica crear un único punto de acceso para todos nuestros datos, de manera tal que si ésta es descifrada, robada o vulnerada, la extensión del daño puede ser bastante grande.
2. E**stablece contraseñas fuertes para acceder a tus cuentas de usuario.** Una contraseña fuerte tiene entre otras, las siguientes características:
    - Más de 8 caracteres
    - Mezcla de caracteres alfabéticos y no alfabéticos
    - No derivarse de información personal (nombre, número de teléfono, número de identificación, fecha de nacimiento, etc.) del usuario o de algún pariente cercano.
3. **Combina mayúsculas, minúsculas y símbolos en una contraseña.**Este sencillo método ayuda a prevenir el

llamado “ataque por diccionario”, el cual es un tipo de ataque por fuerza bruta, en el que hackers utilizan un software especial que en segundos intenta dar con la clave adecuada probando diversas palabras recogidas en un diccionario idiomático.

4. P**ersonaliza las contraseñas que nos asignan por defecto.** Por ejemplo, asegurarnos de que el router -dispositivo que, mediante una red, proporciona conectividad inalámbrica de Internet-, tenga una contraseña segura, ya que es muy probable que la clave que esté designada por defecto para este dispositivo esté publicada en internet. Se debe tener presente que a través del router se puede acceder a todos los dispositivos conectados a su red, los que podrían quedar comprometidos si la contraseña es débil.
5. **Utiliza recursos nemotécnicos.** Esta técnica es muy sencilla y consiste en tomar una frase que te sea fácil de recordar, como por ejemplo de una película o de una canción, y construir la contraseña con la primera letra de cada palabra de la frase. Otra alternativa, consiste en combinar dos palabras y alternar sus letras.
6. **Utiliza gestores de contraseñas.** Un gestor de contraseñas es un programa que permite la generación automática de claves complejas para acceder a distintos recursos. Muchos gestores cuentan con autenticación de doble factor, es decir, añaden una capa adicional de seguridad para acceder a tus datos (por ejemplo, el envío de un SMS que genera un código). Esta última funcionalidad, es una herramienta que nos permite prescindir de dejar las contraseñas guardadas en los navegadores.

Recomendaciones para la protección de contraseñas:

1. **No reveles ni compartas de ninguna forma tus contraseñas.** Son estrictamente personales e intransferibles. No las divulgues por teléfono, ni la

anotes por correo electrónico, o a través de cualquier plataforma o red social, o de cualquier otra forma a nadie.

2. **Presta atención cuando accedes a los servicios desde espacios públicos.** En este aspecto, existen programas que facilitan la interferencia de las plataformas y pueden almacenar las pulsaciones del teclado.
3. **No utilices la opción de "guardar contraseña" en el navegador, para no reintroducirla en cada conexión.** Resulta fácil conseguir estas credenciales, ya que cualquier persona con acceso al ordenador podría consultar las contraseñas introducidas, en la configuración del navegador.
4. **Mantén los sistemas operativos, softwares y aplicaciones actualizados**, para evitar la intromisión en los mismos, mediante ataques cibernéticos. Cada actualización incluye nuevas soluciones a las vulnerabilidades y no invertir el tiempo en instalarlas puede generar una puerta de entrada a diversos tipos de hackers.
5. **Presta atención periódicamente a tus contraseñas, esto es, cámbialas cada cierto tiempo.** Esto cobra importancia en aquellos casos en que se intenta obtener tu contraseña bajo ataques de "brute force" (esto es, utilizando la técnica de ensayo y error, a través de un software que descifra claves empleando una sucesión de varias combinaciones de caracteres compuestos por dígitos, espacios y letras), ya que, al cambiarla, las combinaciones probadas por el ciber atacante quedan sin efecto.