

Este fin de semana hemos sufrido una violación de seguridad provocada por un ataque a los servidores de almacenaje de datos de carácter personal. Como consecuencia de este incidente se puede haber visto comprometida la seguridad de cierta información personal de nuestros clientes. Dependiendo de los casos, los datos afectados pueden ser más o menos sensibles: nombre, apellidos, dirección postal, teléfono, correo electrónico, número de documento de identidad, fecha de nacimiento, nacionalidad, código IBAN de la cuenta corriente o numeración de la tarjeta de crédito.

La transparencia en todas las relaciones que mantenemos con nuestros clientes en el marco de nuestra actividad es uno de nuestros valores fundamentales, por ello, en PTV estamos decididamente comprometidos con la privacidad y seguridad de nuestros clientes, de tal manera, que desde el momento que tuvimos conocimiento de esta situación adoptamos las medidas de protección técnicas y organizativas para poner remedio a la violación de la seguridad de los datos personales, procediendo de inmediato al corte del acceso a los sistemas de la compañía.

De igual manera, hemos procedido a activar un protocolo de actuación para informar, a la mayor brevedad posible, a los clientes afectados, de las medidas de prevención y consejos de seguridad para evitar cualquier problema derivado de esta acción delictiva.

A la misma vez, desde el momento que conocimos la violación de seguridad, hemos sido los principales interesados en esclarecer los hechos. En tal sentido, hemos notificados a la autoridad de control competente, AEPD, la violación de la seguridad de los datos personales dando por ello cumplimiento a lo establecido en el artículo 33.1 del reglamento (UE) 2016/779 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como, a la Guardia Civil a través de la presentación de la correspondiente denuncia.

Como existe el riesgo de que la información afectada pudiera ser empleada con fines maliciosos o ilegales puntualizamos algunas cuestiones y consejos que pueden ser de utilidad en relación a este incidente.

1-¿Cómo sé si mis datos están entre los publicados?

Solo estarían afectados ciertos datos personales de aquellos clientes que hayan recibido comunicación al respecto por parte de PTV ya sea por SMS o Email.

2-¿Cuáles son los datos que pueden haber sido comprometidos?

En la comunicación que el cliente haya recibido por parte de PTV se han identificado los datos afectados por este incidente dependiendo de cada caso. Estos pueden ser datos identificativos o de facturación.

3-¿Entre esos datos está mi cuenta bancaria o tarjeta de crédito?

Si así es, aparecerá explícitamente en la comunicación que ha recibido el cliente.

4-¿Cómo puede afectarme este acceso no autorizado a la información?

Son varios los usos que con fines maliciosos o ilegales, se podrían llevar a cabo debido a la naturaleza de la información. En casos leves se podría utilizar para enviar publicidad sin el consentimiento de la víctima. Entre los casos de mayor gravedad se incluyen, vender estos datos a terceros, realizar una suplantación de identidad o estafa a nombre de la persona afectada e incluso robar dinero con la información obtenida de su cuenta bancaria o sus tarjetas de crédito.

5-¿Qué debo hacer para evitarlo?

Desde PTV le recomendamos que siga los siguientes consejos de seguridad:

- No responda a ninguna petición de información por correo electrónico o teléfono cuyo origen no sea confiable.
- No haga clic en enlaces incluidos en mensajes de correo electrónico, mensajes de Whatsapp, mensajes SMS o MMS cuyo origen no sea confiable.
- Extremar la precaución sobre cualquier transacción o comunicación que pudiera recibir y asegurarse sobre su veracidad durante los próximos meses.
- En el caso de que su código IBAN o número de tarjeta de crédito se haya visto afectado, contactar con su banco y explicarle lo sucedido para que pueda tomar las medidas oportunas.
- En caso de detectar cualquier otra actividad sospechosa, denunciar a la policía y/o consultar al INCIBE (Instituto Nacional de Ciberseguridad) a través del siguiente enlace:

<https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>

6-¿Qué medidas ha implementado PTV para poner remedio a esta violación de seguridad y mitigar sus efectos?

Para remediar esta violación de seguridad y minimizar sus efectos, PTV procedió de inmediato al corte del acceso a los sistemas de la compañía desde el momento en que tuvo conocimiento del ciberataque.

7-¿Cómo puede haber visto comprometida la información de quien no es cliente de PTV?

Todos los datos afectados provienen de la interacción que PTV tiene o ha tenido con estos usuarios como consecuencia de su actividad comercial.

8-Consejos y medidas de seguridad generales para proteger tus datos

- Nunca proporcionar información privada y sensible como el pin de la tarjeta de crédito o las claves de acceso a plataformas o servicios, si es solicitada a través de correos o mensajes cuyo remitente no esté claramente y debidamente identificado.
- No acceder a sitios no seguros ni abrir enlaces en mensajes de correo electrónico o SMS, a no ser que se tenga plena confianza sobre su origen.
- Cambiar las claves de acceso si entendemos que estas pueden haberse visto comprometidas.
- Contactar con su entidad bancaria en el caso de detectar cualquier anomalía.
- Mantener su equipos adecuadamente protegidos con las aplicaciones de seguridad y las actuaciones recomendadas por el fabricante.
- Denunciar ante las fuerzas de seguridad del estado si tienes sospechas razonables de robo de identidad o suplantación.