

Aviso de seguridad y privacidad

Esta semana hemos notificado a un número reducido de clientes empresas, autónomos y particulares un **incidente de datos** como resultado de un acceso no autorizado a los sistemas de uno de nuestros colaboradores. Como parte de este incidente, es posible que se haya **accedido a datos personales de un número limitado de clientes. No hay contraseñas afectadas.**

En cuanto tuvimos conocimiento del incidente, trabajamos con el colaborador para **estabilizar la situación y activar las medidas de refuerzo necesarias en los sistemas informáticos**. Además, hemos activado los protocolos externos e internos existentes, que incluyen la comunicación a los potencialmente afectados, para que activen las medidas de protección necesarias. Vodafone se toma muy en serio la transparencia, así como la comunicación, en materia de seguridad. De esta forma, se ha notificado el incidente al INCIBE (Instituto Nacional de Ciberseguridad de España), a la AEPD (Agencia Española de Protección de Datos) y a los potencialmente afectados, en cumplimiento de la normativa de protección de datos personales. Asimismo, **velamos por la seguridad y privacidad** de los datos y contamos con un experimentado equipo internacional de profesionales de la ciberseguridad que vigilan constantemente la red y los sistemas para garantizar la protección de los datos.

Para más información, se facilitan los siguientes medios de contacto. Para empresas y autónomos: número 22122 (900 878 488 si llamas desde teléfono no Vodafone); para Particulares: número 900 851 151.

Consejos y medidas de seguridad para proteger tus datos

- 1.- No abras enlaces extraños o de fuentes poco fiables incluidos en mensajes de correo electrónico o SMS.
- 2.- Ten especial precaución con los correos electrónicos o mensajes de telefonía que no cuenten con una identificación clara del remitente, particularmente si solicitan información reservada, como tu número de cuenta corriente, datos de tarjetas de crédito, o claves de acceso a plataformas y servicios.
- 3.- Cambia las claves de acceso a servicios y plataformas que se encuentren en activo.
- 4.- Ponte inmediatamente en contacto con tu Banco en el caso de detectar alguna anomalía.
- 5.- Si tiene sospechas razonables de robo de identidad o suplantación, INCIBE pone al servicio del ciudadano el teléfono de consulta 017 o en www.incibe.es/linea-de-ayuda-en-ciberseguridad.
- 6.- No facilites tu contraseña o tu PIN, desde Vodafone nunca te solicitaremos esta información por SMS, llamada o correo electrónico.

Q&A

¿Cómo puedo saber si estoy afectado?

Sólo están potencialmente afectados los que han recibido un SMS informativo o e-mail de Vodafone.

¿Qué datos se han visto comprometidos?

Si eres empresa y éstas potencialmente afectado porque has recibido una comunicación de Vodafone: los datos posiblemente afectados son nombre, CIF, número de contacto, correo electrónico, dirección y cuenta bancaria del cliente empresa. En relación con el autorizado de la empresa, los datos potencialmente afectados son nombre y apellidos, número de contacto y copia del DNI del autorizado de la empresa.

Si eres autónomo y éstas potencialmente afectado porque has recibido una comunicación de Vodafone: los datos posiblemente afectados son nombre, apellido, DNI, número de contacto, correo electrónico, dirección y cuenta bancaria del autónomo.

Si eres particular y éstas potencialmente afectado porque has recibido una comunicación de Vodafone: los datos posiblemente afectados son los datos del DNI, teléfono de contacto, correo electrónico, cuenta bancaria y número contratado. **En caso de que seas cliente prepago, tu cuenta bancaria no se encuentra afectada.**

¿Se ha filtrado información como mis llamadas o mensajes?

No, no se ha visto afectada otra información como las credenciales de usuario y contraseñas o información de llamadas, mensajes, o navegación web.

¿Cuáles son las posibles consecuencias de este incidente?

Debido a la naturaleza de la información afectada, podría utilizarse para tratar de obtener más información de los afectados o con fines fraudulentos. Como medida de precaución, aconsejamos que estén atentos y no accedan a sitios no seguros, y que no respondan a las solicitudes por SMS o teléfono de sus credenciales o cualquier otro dato personal. También le animamos a que compruebe la autenticidad de dichas solicitudes antes de responder. Por ejemplo, la consecuencia más habitual en este tipo de incidentes es que se intente realizar un phishing para posteriormente realizar actividades fraudulentas.

En caso de que en las próximas semanas alguien suplante mi identidad, ¿qué puedo hacer?

Si en las próximas semanas detecta que su identidad ha podido ser suplantada, presente la correspondiente denuncia ante la Policía Nacional o la Guardia Civil y ponga en su conocimiento el incidente comunicado por Vodafone por si tuviera relación con esta posible suplantación. También puede ponerse en contacto con su entidad bancaria por si, de acuerdo con las políticas o recomendaciones de su banco, fuera necesario el bloqueo o cancelación de sus cuentas.

¿Qué medidas se han adoptado como consecuencia del incidente?

En cuanto tuvimos conocimiento del incidente, trabajamos con el colaborador para estabilizar la situación y activar las medidas de refuerzo necesarias en los sistemas informáticos. Además, hemos activado los protocolos externos e internos existentes, que incluyen la comunicación a los clientes por SMS y correo electrónico, para que activen las medidas de protección necesarias.

¿Si no soy cliente cómo es posible que Vodafone tenga toda esta información personal?

Los datos que han podido verse afectados por la filtración debido al acceso no autorizado a las bases

de datos de uno de nuestros colaboradores corresponden a la actividad comercial realizada por la compañía, y en ese ámbito es como se habría recopilado la información.