Un nuevo caso de phishing masivo ataca a las empresas

Alerta por un nuevo caso de "phishing" mediante el envío de correos electrónicos falsos en los que, bajo la apariencia de la Agencia Tributaria y a través de un formulario muy similar al utilizado por este organismo con su logo e imagen institucional, se solicitaba información privada a los destinatarios.

Este comunicado masivo informa a los destinatarios de una falsa notificación pendiente de apertura, solicitando el correo electrónico y su contraseña como datos necesarios para la gestión, con la finalidad de hacerse con el control de la cuenta de correo electrónico de la víctima.

Esta clase de ataques, que se denominan vulgarmente como “phishing”, utilizan la ingeniería social para intentar obtener información privada. Captan la atención del destinatario del correo simulando la apariencia de algún servicio u organismo conocido (Administración pública, bancos, proveedores, etc.) con el fin de redirigirnos a sitios web fraudulentos y obtener información privada.

Consejos para evitar ser víctima de phishing

Crea una cultura de la privacidad dentro de la organización. Forma a los empleados con acceso al correo electrónico para que realicen un uso seguro de esta herramienta.

Sospecha de correos electrónicos que aparenten ser de entidades bancarias u organismos conocidos que soliciten información adicional o credenciales de acceso. Consulta esta clase de correos con la entidad emisora antes de facilitar los datos.

Sé precavido si el mensaje contiene errores gramaticales.

Desconfía de las comunicaciones recibidas desde dominios tipo @gmail, @yahoo u otros similares. Los servicios con cierto prestigio utilizan sus propios dominios corporativos.

Revisa que el texto del enlace contenido en el correo electrónico coincide con la dirección a la que apunta.

¿Cuándo y cómo comunicar un incidente de seguridad? Cinco claves para entender esta obligación

Una de las grandes novedades que trajo el Reglamento General de Protección de Datos en su entrada en vigor el pasado 2018 fue la de comunicar las brechas de seguridad a los interesados que se vean afectados por la misma, cuando sea probable que la brecha entrañe un alto riesgo para sus derechos y libertades.

Por esta razón, los últimos años hemos conocido noticias de violaciones de seguridad que han sufrido algunas empresas que afectan a miles o incluso millones de personas, que con la normativa anterior no hubiesen salido a la luz. Uno de los últimos casos fue el de Orange España, que comunicó una brecha de seguridad sufrida por uno de sus proveedores que afectó a sus propios clientes, exponiendo nombres, apellidos, direcciones postales, teléfonos, correos electrónicos, números de documentos de identidad y fechas de nacimiento.

Aunque en los medios de comunicación se pone el foco en las grandes multinacionales, la obligación de comunicar las brechas de seguridad a los clientes y otros interesados afecta a todas las organizaciones que traten datos de carácter personal, por lo que

ofrecemos las cinco claves para conocer esta obligación:

Cuando comunicar una brecha de seguridad

El Reglamento General de Protección de Datos prevé en su artículo 34 la obligación de comunicar a los interesados cualquier violación de la seguridad cuando esta entrañe un alto riesgo para los derechos y libertades de las personas físicas. Por ende, se debe valorar cualquier incidente que conlleve la destrucción, pérdida, alteración o acceso no autorizados a los datos personales de una organización.

El responsable del tratamiento debe comunicar esta brecha de seguridad sin dilación indebida desde que tenga conocimiento de que se ha producido.

Por qué realizar esta comunicación

La finalidad de esta comunicación es proteger a las personas ante las consecuencias de una brecha de datos personales (por ejemplo, suplantación de identidad, revelación de datos de personales…). Conocer esta información puede ayudar a los interesados a prever las consecuencias y mitigar sus efectos.

A quién realizar la comunicación

Se debe comunicar a todos los afectados por el incidente que haya causado la brecha de seguridad, por ejemplo, clientes, empleados, proveedores o contactos comerciales de la organización.

Cómo realizar esta comunicación

Será necesario realizar la comunicación a cada uno de los afectados, por ejemplo, mediante correo electrónico, SMS o correo postal, entre otros medios. Si supone un esfuerzo desproporcionado o se desconoce con precisión quién ha podido verse afectado, se puede realizar un comunicado público que tenga la misma eficacia.

Qué debe contener este comunicado

Se debe informar a los afectados de la naturaleza del incidente en un lenguaje claro y sencillo, describiendo qué a ocurrido, qué datos se han visto afectados y qué consecuencias puede tener. Además, se deben comunicar las medidas tomadas por el responsable para solucionar la brecha y minimizar las consecuencias, facilitando un medio de contacto para ampliar la información.

Sancionan a la discoteca Fabrik por enviar publicidad a un usuario tras solicitar la baja de sus datos

La discoteca madrileña envió varios mensajes de texto (SMS) con contenido publicitario a un interesado que, molesto por recibir tantas comunicaciones comerciales, solicitó la baja a través de los medios facilitados por el responsable.

Al intentar gestionar la baja desde su propia cuenta de usuario, el sistema no permitió la gestión efectiva de dicha solicitud. Por esta razón, se dirigió al correo electrónico que la discoteca facilitaba a los usuarios para ejercer sus derechos de protección de datos. No obstante, tras solicitar la eliminación de sus datos, el interesado siguió recibiendo comunicaciones comerciales, por lo que decidió interponer una reclamación ante la Agencia Española de Protección de Datos (AEPD), facilitando como prueba todas las comunicaciones recibidas, así como el escrito para solicitar la baja de sus datos.

Actualmente se denomina “spam” a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por “spam” cualquier mensaje no solicitado y que, normalmente, tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada es el correo electrónico. Esta conducta

es particularmente grave cuando se realiza en forma masiva.

El envío de mensajes comerciales sin el consentimiento previo está prohibido por la legislación española. El bajo coste de los envíos de correos electrónicos vía Internet o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades que ofrece en cuanto al volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (denominada LSSI por sus siglas), en su artículo 21.1, prohíbe de forma expresa "el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas". Es decir, se desautorizan las comunicaciones comerciales dirigidas a la promoción directa o indirecta de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, sin consentimiento expreso del destinatario.

Por todo lo anterior y tras realizar las labores de inspección, la AEPD vio acreditados los hechos descritos por el reclamante, por lo que decidió sancionar a CITY OF SOUND 2010, sociedad propietaria de Fabrik, con una multa de 800€ por la infracción del artículo 21 de la LSSI.

La AEPD sanciona a una Federación manchega por realizar pruebas COVID sin informar a los deportistas

La Federación de Deportes para Personas con Discapacidad Intelectual de Castilla-La Mancha (FECAM) ha sido sancionada por la Agencia Española de Protección de Datos (AEPD) con una multa de 3600 euros por realizar test de antígenos sin informar debidamente a los interesados del tratamiento de sus datos personales.

Esta sanción, (que fue reducida por pago voluntario, pues inicialmente la AEPD estimó imponer una multa de 6.000 euros), fue motivada por la denuncia de una usuaria, que vio vulnerados sus derechos al no recibir la suficiente información del tratamiento de sus datos de salud.

En sus alegaciones, la Federación afirmó que sí que se informaba a los interesados del tratamiento de sus datos personales mediante la firma de un protocolo específico, que debía de ser firmado por todos los participantes en las competiciones deportivas. No obstante, según el criterio de la AEPD, este documento no informaba sobre el tratamiento concreto de datos de salud con respecto a las pruebas de antígenos para la detección de la COVID 19 en las competiciones, a pesar de que sí existía un apartado en el que se solicitaba autorización para que la FECAM tratase datos con la finalidad de gestionar un control médico y psicológico para asistir a los deportistas.

Esta Agencia ha subrayado que la pertenencia a una federación deportiva legitima el tratamiento de los datos con la finalidad de promocionar y extender la actividad deportiva correspondiente, pero no para el tratamiento de los datos de salud con fines de control y prevención de la COVID 19, para lo que se precisa una base legal adicional.

Editado por Microlab Hard

Madrid. C/ Cronos 8, 1º, Madrid

Barcelona. C/ Santiago Rusiñol 8, Molins de Rei