Dreamstime

Usar la misma contraseña en varias páginas web puede hacer a un usuario culpable de un uso fraudulento de sus datos por parte de un ciberpirata.

CIBERESTAFAS

Culpable de facilitar un hackeo por usar la misma contraseña

La AEPD considera negligente la actuación de un usuario de Glovo por tener la misma clave en varios servicios que habían sido ciberatacados.

Laura Saiz. Madrid

"¡Hola A.A.A.! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este *email* confirmando la baja y gestionaremos tu petición a la mayor brevedad posible". Con este mensaje automático iniciaba así Glovo una cancelación de su sistema a petición de un usuario, que meses después volvió a ponerse en contacto con la compañía por recibir en su correo la confirmación de un pedido que él nunca había realizado.

Este incidente hizo que Glovo etiquetara la cuenta como fraudulenta y le devolviera el dinero incorrectamente cobrado. Sin embargo, el afectado decidió denunciar el caso ante la Agencia Española de Protección de Datos (AEPD) al entender que el servicio de mensajería estaba tratando sus datos personales de manera ilícita tras su solicitud de baja del servicio.

Sin embargo, una reciente resolución del organismo no le da la razón y archiva el caso, ya que "no ha podido acreditarse debidamente en el expediente que la supresión solicitada por el reclamante no hubiera sido atendida correctamente y se hubiesen continuado tratando los datos personales del reclamante careciendo de base jurídica que legitimara tal tratamiento". No en vano, la defensa legal de Glovo –completada con una visita presencial de la AEPD– demostraba que, tras esta sucesión de hechos, se escondía el *modus operandi* habitual de ciberdelincuentes de Europa del Este, que suplantan la identidad de usuarios de Internet para realizar compras fraudulentas tras determinados y sucesivos ciberataques que van enriqueciendo el mercado negro de datos personales.

Ojo con los robos masivos

"Es raro que haya alguna cuenta habitual de Gmail, Hotmail u otras que no hayan sido comprometidas varias veces, por lo que cabe suponer que la mayoría de nuestros datos de correos y contraseñas, si no se cambian, están en bases de datos, que además pueden haber sido enriquecidas con información de tarjetas o redes sociales". De esta manera alerta Alexander Benalal, socio de ThinkSmartLaw, del peligro de no responder adecuadamente a un ciberataque masivo y usar las mismas contraseñas en diferentes páginas, ya que esto facilita a los piratas informáticos acceder a los datos en distintas web.

Los piratas informáticos llegaron a recabar varios datos personales del afectado

"La AEPD dice que el reclamante fue negligente al utilizar reiteradamente la misma clave en distintos servicios que fueron afectados por una brecha de seguridad que dejó expuestas sus credenciales (aparentemente, en su caso, de Dropbox)", según explica Alexander Benalal, socio de ThinkSmartLaw y experto en nuevas tecnologías. Estos datos se fueron enriqueciendo en otros hackeos, hasta permitir a los ciberdelincuentes tener su ubicación geográfica, datos de empleo, números de teléfono, perfiles en redes sociales y tarjetas de crédito. "Es llamativo que, de hecho, en la suplantación de identidad en Glovo no se usó la tarjeta que inicialmente el reclamante tenía inscrita, sino otra suya que es muy posible que proviniese del mercado negro", indica el experto, que incide en que "el perjudicado, por haber usado sus claves en diferentes servicios y no haberlas cambiado, actuó negligentemente facilitando la suplantación de identidad".

Según Benalal, esta resolución de la AEPD "pone en valor una vez más las obligaciones de los usuarios respecto de sus cuentas y claves, no sólo para prevenir ciberataques, sino para no perjudicar sus posibles acciones futuras en caso de sufrirlos". El experto lamenta que "esas obligaciones mínimas de diligencia rara vez se cumplen en el ámbito doméstico (y muchas veces tampoco en el profesional)".

TECNOLOGÍA

El TJUE fija los límites de la extracción de datos de las webs

Víctor Moreno. Madrid

El Tribunal de Justicia de la Unión Europea (TJUE) es el órgano competente para interpretar el Derecho europeo, pero también se ha convertido en un referente sobre cómo aplicar las normas respecto a las nuevas herramientas tecnológicas. El último desarrollo que ha pasado por sus manos es el denominado *web scraping*, que se podría definir como la aplicación de técnicas que permiten la extracción de datos e información de cualquier página de Internet mediante el uso de un *script* o software.

En este caso, el Tribunal Regional de Riga (Letonia) ha planteado una cuestión prejudicial sobre un conflicto entre CV Online, un sitio web con una base de datos en la que aparecen anuncios de empleo, y Melons, una sociedad que explota un motor de búsqueda especializado en este tipo de información. Según explica el fallo del TJUE, el buscador utilizaba un software para buscar palabras clave en los anuncios clasificados y así presentar los mejores resultados. Sin embargo, CV Online estimaba que, al hacer eso, Melons extraía y reutilizaba una parte sustancial del contenido de la base de datos empleada en la página web.

A favor, pero con límites

Finalmente, la corte europea ha apoyado los argumentos de Melons, la empresa que realizaba el *scraping*, lo que según Carlos Rivadulla, abogado de Ecija, representa un respaldo a este tipo de actividad. Sin embargo, al mismo tiempo, el alto tribunal también ha querido utilizar este fallo para ser más preciso en su interpretación y ha fijado una serie de límites que deben cumplirse para no sobrepasar la legalidad.

"Por un lado, la base de datos online que se extracta debe ser accesible libremente en Internet. Por el otro, el fabricante de dicha base de datos podrá oponerse al *web scraping* en la medida en que tales actos ocasionen un perjuicio a su inversión en la obtención, certificación o presentación de dicho contenido. Es decir, siempre que constituya un riesgo para las posibilidades de amortizar la inversión", resume Rivadulla.

Para entender mejor el asunto, el letrado pone el ejemplo de una web de viajes que hace *scraping* de los datos de una compañía aérea para incorporarlos a su sitio. "En este caso, podríamos entender que no se causa un perjuicio a la aerolínea, puesto que dispone y requiere esa información para su propia operativa". "Cuestión distinta", añade Rivadulla, "sería el caso de una empresa que realiza una inversión considerable en obtener unos datos, de los que no dispone ni había creado para su operativa ordinaria, y que un tercero los extractara para crear, por ejemplo, una web competidora".

Dreamstime

El TJUE ha fallado sobre el 'scraping', sistema que permite la extracción de datos de cualquier web.