La ola de hackeos pone en la diana a los ciudadanos: "Viene una campaña de intentos de estafa sin precedentes"

ChatGPT puede usrse para perfeccionar estafas online

Mayo ha sido un mes terrible para la ciberseguridad española. En cuestión de días han caído víctimas de ciberataque, o están investigando supuestas brechas de seguridad, el Banco Santander, Telefónica, Iberdrola, la DGT y la Universidad Complutense. A ellos se suma una brecha internacional que también habría afectado a clientes españoles: la sufrida por Ticketmaster, que incluiría los registros de más de 500 millones de usuarios de su plataforma de entradas en todo el mundo.

Todos ellos han sido ataques para robarles los datos personales de los ciudadanos que almacenaban sus sistemas. Empresas como el Banco Santander o Iberdrola han intentado rebajar la importancia de las brechas alegando que entre la información sustraída solo hay "datos de contacto" y "no contraseñas o información financiera". Sin embargo, especialistas en ciberseguridad desechan ese llamamiento a la calma y recuerdan que estos robos ponen en la diana a los ciudadanos afectados.

"Pueden no tener mis datos bancarios, pero tienen mi DNI, saben que yo pertenezco al Santander o que estoy dado de alta en Telefónica, o que soy cliente de Iberdrola. Con eso ya tienen suficientes datos para elaborar un intento de estafa súper dirigido en el que se hagan pasar por estas empresas para engañarte", avisa Rafael López, experto en ciberseguridad de la firma Perception Point.

"Hay que tener en cuenta que esto ya no lo hace un tío picando piedra y preparando los mails a mano", continúa el especialista: "Este tipo de datos ya se pueden meter en sistemas de inteligencia artificial que te preparan los *phishing* como si fuera una churrera y lo dejan perfecto y personalizado. Por eso es tan peligroso. Ahora lo que hay que alertar es que viene una campaña de intentos de estafa sin precedentes".

Algunas de las campañas de fraudes digitales más exitosas, especialmente las dirigidas contra ciudadanos de a pie, no se basan en romper las defensas de sus dispositivos a base de fuerza bruta informática. Al contrario, lo que intentan es que sea la víctima quien les abra la puerta. Algo que pueden conseguir con un solo dato personal, como sabiendo que su objetivo es padre o madre, o cuál es su entidad bancaria.

Todo el mundo es vulnerable

A esta estrategia los ciberdelincuentes suman una artimaña que puede derribar incluso la defensa más robusta: la sensación de urgencia. Esta semana el experto en ciberseguridad Marc Rivero, uno de los principales especialistas en malware e investigación de amenazas de España, contó en el podcast Securiters como casi cae en un phishing. “Me llegó un mensaje de 'alerta DGT': tienes una multa impagada por valor de 35 euros que se va a duplicar en 24 horas. Debes pagarla ahora”.

“El hecho objetivo es que yo estoy esperando el pago de una multa. Me pilló en medio de una reunión. Lo hice super rápido, estaba liado...”, resume Rivero, que declara que llegó a clicar en el enlace fraudulento y rellenar los campos que le pedían los ciberdelincuentes para pagar la supuesta multa, hasta que se dio cuenta de que no podía identificarse con certificado: “Madre mía si hace 15 años que me dedico a esto y casi caigo en un *phishing...*”.

El aviso del experto destaca que pese a mantener un espíritu crítico en las comunicaciones digitales, los timadores pueden aprovechar cualquier momento de distracción y un golpe de suerte como el hecho de que exista una multa sin pagar (o un dato personal que caiga en sus manos) puede terminar en ciberestafa.

Los proveedores

Algunas de las empresas afectadas por ciberataques esta semana se han excusado alegando que estos no han afectado a sus sistemas sino a los de los proveedores. Tanto Telefónica como Iberdrola han apuntado que los robos han sido a terceras empresas a las que ellas habían cedido las bases de datos con información de sus clientes para que las gestionaran.

Una situación que, para los especialistas, lo que hace es poner el foco en que estas grandes empresas delegaron las bases de datos a compañías con medidas de seguridad menos solidas. “Esa tercera empresa tendría que asumir los mismos protocolos que la que recoge los datos y si hay una filtración, que la responsabilidad la asuman las dos”, pide Rafael López, en referencia a las posibles multas de la Agencia Española de Protección de Datos (AEPD).

“Cuando haya una sanción, que paguen las dos. Es la única manera de que las grandes se pongan las pilas y exijan lo máximo a todas sus subcontratas”, continúa el experto, que pide también al regulador de privacidad que sea más estricto cuando se producen este tipo de brechas, que afectan muy poco a las operaciones de las empresas pero pueden suponer miles de intentos de estafa contra sus clientes.

“Si el organismo que tiene que sancionar lo hace tarde y mal, nunca vamos a dejar de ver este tipo que brechas”, concluye.

Según el Reglamento General de Protección de Datos de la UE, los reguladores de privacidad pueden multar con hasta 20 millones de euros o el 4% de la facturación anual de una empresa, la cifra que sea más alta. Sin embargo, la Agencia Española nunca se ha acercado a esas cifras para las filtraciones de información personal. Su sanción más elevada ha sido contra Google (10 millones de euros en 2022) por su gestión del derecho al olvido. La segunda, contra Vodafone (8 millones en 2021) por la falta de control en el envío de comunicaciones comerciales.

La multa más cuantiosa por una brecha de datos impuesta por la AEDP fue precisamente contra Iberdrola y su filial i-DE Redes Eléctricas Inteligentes (3 millones de euros a la primera y 3,5 millones a la segunda) tras otro grave ciberataque que la compañía eléctrica sufrió en 2022.

En el caso de las instituciones públicas como la DGT o la Universidad Complutense, el regulador de la privacidad ni quiera puede multarlas económicamente. La ley española establece que ninguna sanción contra un ente público puede llevar aparejado este tipo de sanción, sino que debe quedarse en un “apercibimiento”.