¿Qué es el phishing y cuáles son sus consecuencias?

Helena Sassoli

El phishing es un tipo de ataque de ingeniería social que se utiliza a menudo para robar datos de los usuarios, incluyendo credenciales de acceso y números de tarjetas de crédito. Se produce cuando un hacker, haciéndose pasar por una entidad de confianza, engaña a la víctima para que abra un correo electrónico, un mensaje instantáneo o un mensaje de texto. La mayoría de los ataques de phishing acaban convirtiéndose en una brecha de seguridad que causa graves daños a las personas al dejar sus datos personales completamente comprometidos.

No todos los ciberataques tienen éxito, pero los que lo consiguen suelen tener consecuencias catastróficas tanto para las organizaciones como para sus clientes.

El ciberataque más común es el "*phishing*" o suplantación de identidad, término que denomina un modelo de abuso informático que se comete mediante el uso de ingeniería social y se caracteriza por intentar adquirir información confidencial de forma fraudulenta.

El objetivo principal de este tipo de ataque cibernético es la obtención de datos valiosos como contraseñas, información bancaria, etc. y el *modus operandi* suele ser siempre el mismo: el cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea, solicitando información o la realización de un pago pendiente.

El auge de *phishing* es un claro síntoma del cambio de tendencia que estamos observando en el escenario internacional del cibercrimen. Nos encontramos con menos ataques dirigidos a tecnología, y más ataques dirigidos hacia personas. El motivo es sencillo: el cibercriminal cuenta con que siempre hay una víctima desinformada, o suficientemente distraída como para no prestar la atención necesaria a los correos electrónicos o mensajes que recibe. Las empresas cada vez invierten más en tecnología de seguridad y, sin embargo, el eslabón más débil sigue siendo el factor humano.

Aunque el *phishing* masivo (envío de correos genéricos a un gran número de objetivos con la esperanza de que al menos algunos caigan en el engaño), sea el ataque más frecuente, el tipo de ciberataque más eficaz es sin duda el conocido como *spear-phishing*. Este suele materializarse en un email personalizado y dirigido específicamente a la persona concreta que lo recibe, que usa información, normalmente obtenida por ingeniería social o fuentes abiertas, para aumentar la sensación de que ese email procede de la fuente que se está intentando suplantar. Además, si se habla de "alerta", "urgencia" o "importancia" el receptor derivará su atención hacia el tema en sí y bajará la guardia respecto de la credibilidad del remitente.

En 2021 más de la mitad (54%) de los ataques de phishing que tuvieron éxito terminaron en una violación de los datos de los clientes, y el 48% acabó con las credenciales y cuentas comprometidas.

Pues bien, como anticipábamos al principio del artículo, las posibles consecuencias de los ciberataques pueden ser nefastas para las compañías que sufren dichos ataques.

Según un informe de Proofpoint (*State of the Phish Report 2022*), realizado mediante una encuesta con 600 profesionales de seguridad de TI de Australia, Francia, Alemania, Japón, España, Reino Unido y Estados Unidos, en 2021 más de la mitad (54%) de los ataques de *phishing* que tuvieron éxito terminaron en una violación de los datos de los clientes, y el 48% acabó con las credenciales y cuentas comprometidas. En general, el 83% de las organizaciones informaron que han experimentado un ataque de *phishing* con éxito en 2021.

Las violaciones de datos de clientes, o brechas de seguridad, representan un daño devastador para las empresas, al quedar expuestos a todo tipo de uso los datos de sus clientes. Un claro ejemplo de lo anterior es el incidente de seguridad sufrido por Uber, la empresa americana que hizo realidad la simple idea de conseguir un medio de transporte pulsando un botón. A principios del pasado mes de septiembre de 2022, según la información filtrada y no confirmada por la compañía, Uber sufrió una brecha de seguridad como resultado de un ataque de ingeniería social dirigido contra uno de los empleados, a través del cual los hackers habrían conseguido acceso a su cuenta en Slack, el servicio de comunicación que emplean a nivel interno, y de ahí a los sistemas internos de Uber. Nada nuevo para Uber: ya en el año 2017, la compañía admitió haber sufrido un ciberataque que afectó a 57 millones de clientes y conductores. Ejemplos de brechas de seguridad, por desgracia, tenemos muchos: en diciembre de 2019, la propia Microsoft, una de las empresas que más datos de usuarios tiene en sus registros, fue hackeada, quedando expuestos los datos de hasta 250 millones de usuarios; en septiembre de 2018, un fallo en Facebook expuso las fotos privadas de casi 7 millones de usuarios durante doce días; suma y sigue.

No todos los ciberataques tienen éxito, pero los que lo consiguen suelen tener consecuencias catastróficas tanto para las organizaciones como para sus clientes.

Si no se toman a tiempo medidas adecuadas, las violaciones de seguridad de los datos personales pueden entrañar graves daños y perjuicios para las personas físicas, tales como la pérdida de control sobre sus datos personales, la restricción de sus derechos, discriminación, usurpación de identidad y pérdidas económicas.

Por ello, la empresa, responsable del tratamiento de los datos personales, cuando tenga conocimiento de que se ha producido una violación de seguridad, tiene que proceder a notificar la misma a la autoridad de control competente a la mayor brevedad, y tomar todas aquellas medidas de "contención" apropiadas.

Si no se toman a tiempo medidas adecuadas, las violaciones de seguridad de los datos personales pueden entrañar graves daños y perjuicios para las personas físicas, tales como la pérdida de control sobre sus datos personales, la restricción de sus derechos, discriminación, usurpación de identidad y pérdidas económicas.

Pero, como siempre, prevenir es más importante que curar. Por ello, es conveniente que las compañías tomen las precauciones necesarias para evitar que posibles ciberataques encuentren terreno fértil entre sus empleados. Las reglas de oro que nunca está de más recordar son: (i) utilizar contraseñas distintas para cada servicio o aplicación; (ii) prestar mucha atención al contenido sospechoso en los emails y tener en cuenta el nombre del remitente en los correos electrónicos; (iii) proteger los ordenadores/móviles con un software de seguridad; y (iv) proteger los datos haciendo una copia de seguridad que no estén conectada al servidor de la compañía.