ECIJA
Calle Serrano 69, 28006 Madrid
Tel: +34 917 816 160
www.ecija.com

Que este verano no te pesquen

Natalia Antúnez, senior de privacidad y protección de datos

En esta época del año cuando las vacaciones de verano están a la vuelta de la esquina y estamos pensando en la merecida desconexión mientras realizamos tareas de nuestro día a día, es cuando los atacantes están más al acecho, esperando un descuido de cualquier empleado.

El conocido ataque *phishing* es aquél a través del cual, por medio de un correo electrónico malicioso (en el que el autor se hace pasar por una empresa legítima existente o una persona de confianza), o una página web (generalmente clonada de una existente para tener más credibilidad), se intentan obtener datos confidenciales, entre los más populares y más impacto pueden causar, credenciales de accesos a sistemas, números de cuenta bancaria y claves bancarias, el número de DNI, junto con otros datos asociados al mismo. Una vez el atacante obtiene dicha información, el alcance de los daños y la repercusión puede ser amplia. En este sentido, es importante tener en cuenta que por parte de los atacantes no hay distinciones, por ello, ya sea el empleado un becario recién llegado a la organización, un directivo, CEO de la entidad o un externo, puede ser objeto de recibir estos correos electrónicos, con el fin de poder obtener la información de interés para el atacante y poder llegar incluso a acceder al hueso de las organizaciones, pudiendo causar daños tanto con respecto a la confidencialidad, como integridad e incluso disponibilidad de la información confidencial de la organización.
Hace años los correos maliciosos eran evidentes, dado que se utilizaban correos cuestionables, la traducción utilizada no era correcta, incluso el nombre utilizado para dirigirse a los destinatarios no correspondía con estos. si bien en la actualidad, los ataques son más sofisticados, llegando incluso a utilizar el dominio de empresas reales, o incluso de la propia empresa, dando apariencia de pertenencia a la organización. En este último caso, si la empresa es pequeña y todos los empleados se conocen, este aspecto no tendría mucho impacto, puesto que las alarmas pueden saltar, pero en caso de recibir un email del "departamento de recursos humanos" o "contabilidad" desde un correo corporativo, para completar un cuestionario o acceder a un archivo, el riesgo es mucho mayor y las posibilidades de éxito de los atacantes son más que considerables.

Las consecuencias para cualquier entidad que sufre un phishing son muy variadas, como:

- Robo de documentos confidenciales, así como de datos personales que pueden estar asociados o incluidos en la propia documentación.
- Pérdida de acceso a contenidos ubicados en dispositivos que son accedidos tras la vulneración de las credenciales de los usuarios.
- Cargos fraudulentos en tarjetas de crédito, así como posibles pagos a través de medios oficiales de la entidad que ha sufrido el ataque.
- Usurpación de la identidad de las personas cuya información es accedida tras el ataque.

Quizá la mayor consecuencia es el incumplimiento normativo que puede derivarse en aquellos casos, en los que no se hayan tomado medidas adecuadas para prevenir este tipo de ataques.

Normativas europeas como la relativa a protección de datos, así como, la relativa a ciberseguridad, (más conocida NIS2), recogen entre sus obligaciones, que las entidades afectadas por estas normas deban establecer procedimientos y medidas de seguridad, con la finalidad de proteger la información que manejan y sus activos, lo cual ayuda a prevenir ataques tales como el phishing.

Estas normas recogen la obligación de notificar a autoridades de control, como la Agencia Española de Protección de Datos, e Incibe, en aquellos casos en los que produzca un ataque o brecha seguridad que afecte a los datos y/o información que manejen las empresas. Como consecuencia de estas posibles notificaciones, puede derivarse peticiones de información de estas autoridades con el fin de valorar si los procedimientos, políticas y medidas de seguridad de la empresa atacada son suficientes para prevenir el ataque, imponiéndose sanciones en el caso de no ser así. Por ello, el incumplimiento de estas normas, no solo facilitan el ataque, si no que puede dar lugar a un incumplimiento normativa.

No obstante, estas amenazas pueden prevenirse revisando, y en su caso, aumentando la seguridad digital de las empresas con el desarrollo de medidas como,

- Establecer una política de usos de medios tecnológicos para empleados.
- Informar a los empleados de la necesidad de verificar siempre el remitente de los correos recibidos y desechar los que sugieran acciones sospechosas.
- Correos con enlaces a webs con dominios diferentes a la denominación de la empresa u organismo oficial remitente.
- Verifica que las páginas webs a las que llegues son seguras y disponen de una dirección HTTPS con un candado gris visible en la barra de direcciones.
- Desconfía de las informaciones profesionales u oficiales que recibas a través de remitentes con extensiones genéricas, dado que, por lo general, las instituciones y organizaciones suelen tener su propio dominio.
- Solo compartir información personal en aplicaciones y plataformas de confianza.
- Mantener tus aplicaciones actualizadas.

Por ello, recomendamos alentar y concienciar a nuestro personal (interno y externo) para tomar las debidas precauciones y cuando estén fuera de la oficina y se conecten desde sus dispositivos móviles, sean cautos.

ECIJA

FT
FINANCIAL TIMES

Most innovative law firm in continental Europe

THE LAWYER

Best European TMT Firm

TOP RANKED Chambers EUROPE

Most recognized Spanish firm in LATAM and Best European TMT Firm

The LEGAL 500

34 practices globally recognized in 10 jurisdictions

Forbes

Best Technology Firm

Most innovative project, Best Digital Economy Firm

Calle Serrano 69
28006, Madrid