INFORMACIÓN IMPORTANTE PARA LAS EMPRESAS!!!

Se ha detectado una campaña de correos electrónicos fraudulentos, de tipo *phishing*, que intentan suplantar a entidades con ofertas de contratación publicadas en la Plataforma de Contratación del Sector Público. En los correos se incluye información que previamente ha sido publicada en dicho portal y solicitan información de facturación para posteriormente proseguir con el ingreso del importe de la factura.

Solución

Si se ha recibido un correo electrónico con las características descritas, pero no se ha dado respuesta, es importante notificar a los responsables de la empresa o al equipo encargado de la seguridad de la información de la entidad para que tomen medidas de concienciación en ciberseguridad con el resto de empleados, y así mantenerse alerta. También es importante que se informe a la empresa suplantada de lo que está sucediendo. Una vez hecho esto, eliminar el correo y marcarlo como no deseado.

En caso de haber dado respuesta al correo con la información que se solicita, es de vital importancia informar al equipo de IT aportando toda la información sobre lo sucedido y al resto de empleados para evitar posibles víctimas al igual que a la empresa suplantada.

Se deberán recopilar las evidencias (por ejemplo, con capturas de pantalla) y contactar con las Fuerzas y Cuerpos de Seguridad del Estado para presentar la correspondiente denuncia. Además, se puede reportar el incidente aquí.

En caso de haber llegado a efectuar el pago de alguna cuantía económica, se deberá contactar con la entidad emisora, a través del departamento correspondiente dentro de la empresa, para que puedan bloquear cualquier transferencia.

El *phishing* es uno de los ciberataques que más afecta a las empresas de todos los tamaños y sectores. Para evitar ser víctima de este tipo de estafas, es esencial que todos los empleados sepan reconocerlo, revisen cuidadosamente los correos electrónicos que solicitan información sensible o pagos y puedan detectar el ataque en sus diferentes formas.

Detalle

Los correos electrónicos detectados simulan provenir de una entidad pública donde se observa una dirección de correo electrónico que no se corresponde con el dominio corporativo, lo que hace sospechar de la veracidad del mismo.

En el cuerpo del correo, se solicita la remisión de facturas, y para dar más credibilidad, utilizan información extraída de la Plataforma de Contratación del Estado, como el número de expediente o el nombre del contrato adjudicado.

De esta forma, los ciberdelincuentes pretenden engañar a las empresas y conseguir que envíen información sensible o, incluso, que redirijan los pagos a cuentas bancarias distintas de las habituales.