



Solicitud de pagos fraudulentos a empresas

La Policía Nacional advierte sobre el "Phising" a empresas, en el cual se recibe un supuesto correo electrónico proveedores o clientes en el cual le solicitan un pago

- El correo procede en apariencia de otra empresa de la que son clientes y en él le informan de un "cambio" en el número de cuenta
- En algunos casos la notificación va precedida por una llamada telefónica en la que un interlocutor informa que han cambiado de entidad bancaria y que remitirá mediante correo electrónico el nuevo I.B.A.N. (Internacional Bank Account Number)
- Se ha dado algún caso en que un supuesto cliente solicitaba el envío de mercancía en un contenedor a un puerto de destino diferente al habitual
- Desde esta Comisaría se recomienda que cuando llegue un correo de ese tipo se contacte telefónicamente con el proveedor o cliente en su caso

14-septiembre-2018.- Varias empresas de Vigo han recibido supuestos correos electrónicos de clientes o proveedores en los cuales solicitaban el abono de una factura real en una cuenta diferente a la habitual.

En uno de estos casos, la factura superaba ampliamente los 300.000 €, y la responsable del área de administración, extrañada por ello, contactó a través del teléfono con la empresa emisora de la factura.

Su cliente negó el cambio de cuenta bancaria y la informó que además esa factura todavía no había sido emitida.

Además se daba la circunstancia que dicha cuenta se correspondía con un banco domiciliado en un paraíso fiscal, lo cual no se coincidía con la política fiscal de esa empresa.

Víctimas en Vigo

Esta no sería la única denuncia en esta Comisaría, ya que pocos días después el responsable de una empresa del sector pesquero se presentó en Comisaría para denunciar que había recibido una carta en la cual un cliente le solicitaba el envío de pescado a un puerto de destino ubicado fuera de las rutas comerciales habituales.

Al hablar con su cliente este le comentó que él no había cursado dicha orden, y que podría tratarse de algún tipo de estafa.

Todo ello generó una serie de contactos desde esta Comisaría con diversas empresas del sector, descubriendo que varias de ellas habían sido contactadas a través de correos electrónicos en los que el emisor se hacía pasar por un cliente o proveedor habitual de la empresa para solicitar el envío de mercancía o bien el pago de servicios.

En todos los casos dichos correos parecían reales y los dominios utilizados por el remitente variaban en un punto o alguna letra con respecto al de la empresa real, e incluso usaban cuentas personales corporativas de empleados de esas empresas con mínimos cambios para que tuviesen apariencia real.

Las cantidades solicitadas varían entre las diferentes empresas y su volumen de negocios, si bien se movían en un abanico de entre los 80.000€ y 1.000.000€.

Para dar mayor confianza en algunos casos se realizaba una llamada previa a la empresa para informarle que les remitirían un correo electrónico con el nuevo número de cuenta.

Recomendaciones

En caso de recibir un correo electrónico en el cual se informa de un cambio en el número de cuenta contactar con el responsable de la empresa vía telefónica, nunca a través del correo electrónico, ya que éste puede estar siendo controlado de modo remoto.

Ha de comprobarse que las direcciones de correo electrónico sean las correctas, ya que a veces puede cambiarse la real que finalice en .com, por una .co.

En otros casos una v puede ser sustituida por una b, o una y por una i, y fonéticamente no los apreciaremos.

Ante cualquier duda debemos contactar con la Policía Nacional, bien personalmente o a través del teléfono 091.