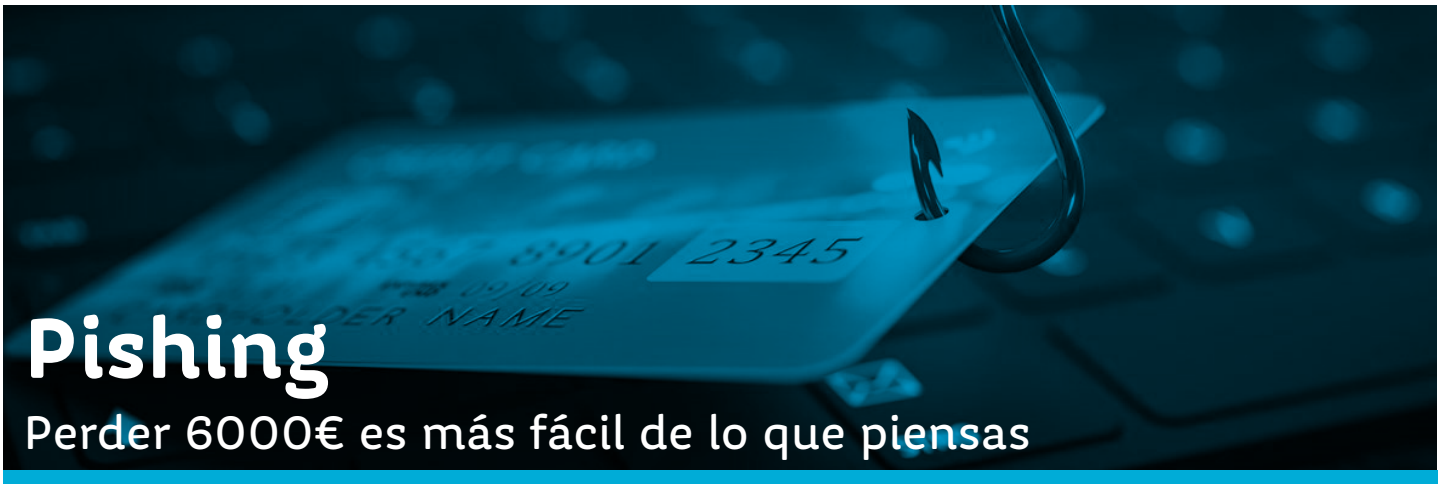

Pishing

Perder 6000€ es más fácil de lo que piensas

Marta es la gerente de una pequeña empresa en la ciudad de Girona. Al ser una estructura familiar, ella misma es quien realiza los pagos a clientes y proveedores. De esta manera, tiene en todo momento el control de la tesorería. Es una tarea delicada y prefiere hacerlo ella misma.

Un día, recibe un correo de su proveedor de e-mail (Gmail, Hotmail o similar) diciéndole que su contraseña había sido expuesta públicamente, y que debería cambiarla de inmediato para garantizar su seguridad. El correo tenía toda la estética de un e-mail oficial (logotipos, tipo de letra, forma del mensaje, color de los botones...) y se fió. Hizo clic y cambió su contraseña.

A estas alturas, el hacker ya tiene su contraseña de correo electrónico y accede a su bandeja de entrada con total libertad.

Después de investigar, detecta un correo electrónico legítimo pendiente por leer de un proveedor. Este le solicita el pago de 6000€, y el mismo e-mail, le indica el número de cuenta donde hacer la transferencia. Esta situación es habitual en muchas pymes, pero... ¿Qué hace el hacker?

Abre el correo del proveedor, lo edita y modifica el número de cuenta. Lo coloca de nuevo en la bandeja de entrada y lo marca como «no leído».

Al día siguiente, Marta accede a su correo y empieza a contestar los correos pendientes. Entre ellos, está hacer el pago de 6000€ a Juan, que es el dueño de la empresa de transportes que envía los productos a los clientes de Marta. La factura es el pago mensual de su servicio. Y ahora viene la secuencia y el desenlace final de la historia:

1. Marta hace la transferencia con total normalidad, pero al día siguiente...
2. Juan le escribe reclamando (de nuevo) el pago.
3. Ella le confirma que está procesado, pero él no ha recibido nada.
4. Al comprobar los números de cuenta... sorpresa, no coinciden.

Marta ha enviado 6000€ al número de cuenta del hacker de manera voluntaria, lo que complica mucho su recuperación. Detectada la estafa, debe cambiar la contraseña de su correo electrónico de inmediato, siempre a través de la web oficial del proveedor. De esta manera, el hacker deja de tener acceso a su número de cuenta.

El siguiente paso, es notificar la incidencia al banco y a la policía.

Articulo publicado en: https://imatica.com/ataque-phishing-caso-real/