Nueva alerta por estafas: Se hacen pasar por Correo Argentino para robar datos de las tarjetas

01/08/2023

Una nueva estafa tomó por sorpresa a miles de argentinos en los últimos días. No se usó una metodología nueva, pero sí un recurso que a veces resulta muy difícil de detectar. Se trata de un nuevo caso de "*pishing*", el engaño a través del cual los delincuentes intentan obtener información confidencial (generalmente los datos de la tarjeta de crédito) haciéndose pasar por una persona o empresa que generalmente interactúa virtualmente con sus clientes.

En este caso, la empresa que sufrió robo de identidad fue **Correo Argentino** y los medios a través de los cuales

intentaron hacer la estafa fueron “SMS” e Internet. El periodista **Oliver Galak** quienvivió la experiencia en “carne propia”, compartió a través de Twitter el detalle de cómo trataron de estafarlo, para tratar de advertir a otras personas.

Además, la propia empresa de correos publicó un aviso en su cuenta para advertir a sus clientes.

Cómo es el engaño

Según explicó Galak, el primer contacto de los “ciber delincuentes” se hace por mensaje de texto al teléfono celular. “Simulan contactarte por un envío de Correo Argentino. Está muy bien hecho; me costó darme cuenta que no era un mensaje oficial”, publicó en sus redes.

El mensaje, según mostró el usuario dice “Argentina – Post – Su paquete tiene una dirección incorrecta y no puede ser entregado. Por favor, visite la página para actualizar la dirección”, a lo que se suma un link que conduce a una web que utiliza el nombre, los colores y la tipografía de Correo Argentino.

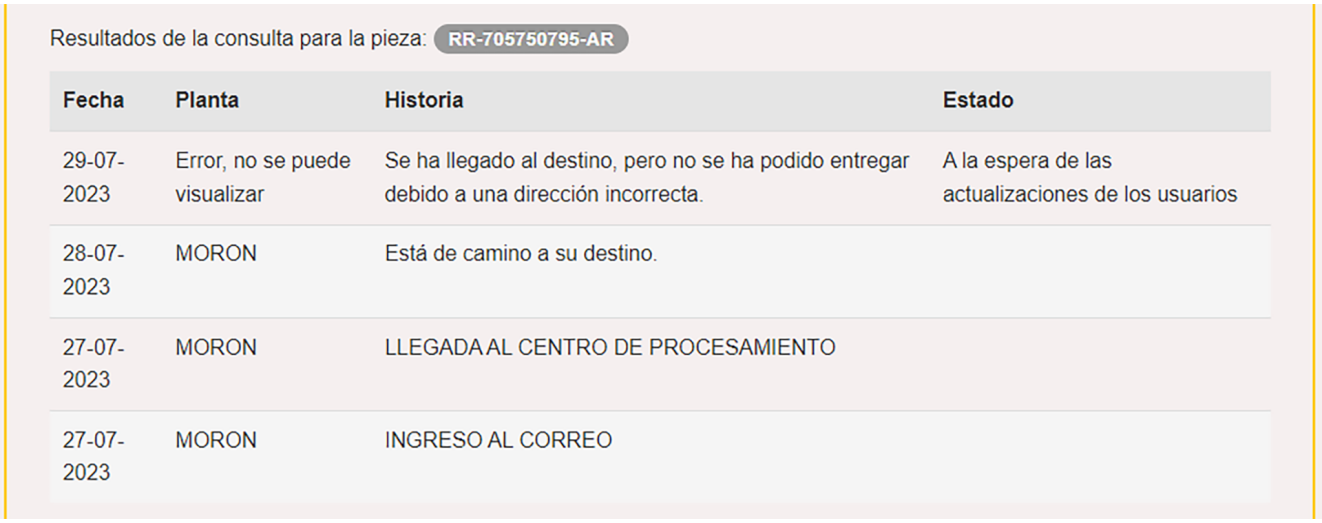
(Fuente)

El sitio, como se puede apreciar en la imagen compartida por el periodista, utiliza incluso un lenguaje similar al de Correo Argentino, por lo que resulta difícil reconocer a simple vista que no se trata del sitio oficial de la empresa.

No obstante, si se observa la barra de dirección, se encuentra que la página que se está visitando es en realidad auuapst.com.

Ahora bien, si se sigue adelante y se presiona en el botón que dice “haga clic para actualizar”, el sitio redirige a una lista de seguimiento falsa, con información perfectamente creíble, pero irreal.

De hecho, Galak detalló que, al menos en su casa, el número de seguimiento que visualizó en la web era real. “Los datos que te copian en el sitio falso tienen algún punto de contacto con el envío real con ese mismo número”, sostuvo.



Resultados de la consulta para la pieza: RR-705750795-AR

Fecha	Planta	Historia	Estado
29-07-2023	Error, no se puede visualizar	Se ha llegado al destino, pero no se ha podido entregar debido a una dirección incorrecta.	A la espera de las actualizaciones de los usuarios
28-07-2023	MORON	Está de camino a su destino.	
27-07-2023	MORON	LLEGADA AL CENTRO DE PROCESAMIENTO	
27-07-2023	MORON	INGRESO AL CORREO	

“Algo que no estoy seguro de si fue adrede o no (pero sospecho que sí): el SMS de la estafa me llegó hoy (30 de julio) a las 12:24. El sitio oficial del Correo no permite verificar el seguimiento de envío los domingos entre las 11 y las 13.30″, contó.

“En cambio, el falso sitio sí funciona, y por lo tanto más de un ansiosos cliqueará en ‘actualizar la dirección de envío’ antes de poder verificar con la plataforma oficial. Hoy en día muchos tienen envíos pendientes que esperan que les llegue”, agregó el periodista.

Cuando se accede a completar la supuesta información faltante, se abre un cuadro de diálogo con algunos datos de contacto, entre los que se encuentran algunos esenciales para el uso online de tarjetas de crédito, como el DNI.

Correo Argentino

Rellene la información correcta

Nombre completo*

DNI*

00.000.000

Dirección de envío*

Dirección 2

Teléfono*

Correo*

Provincias*

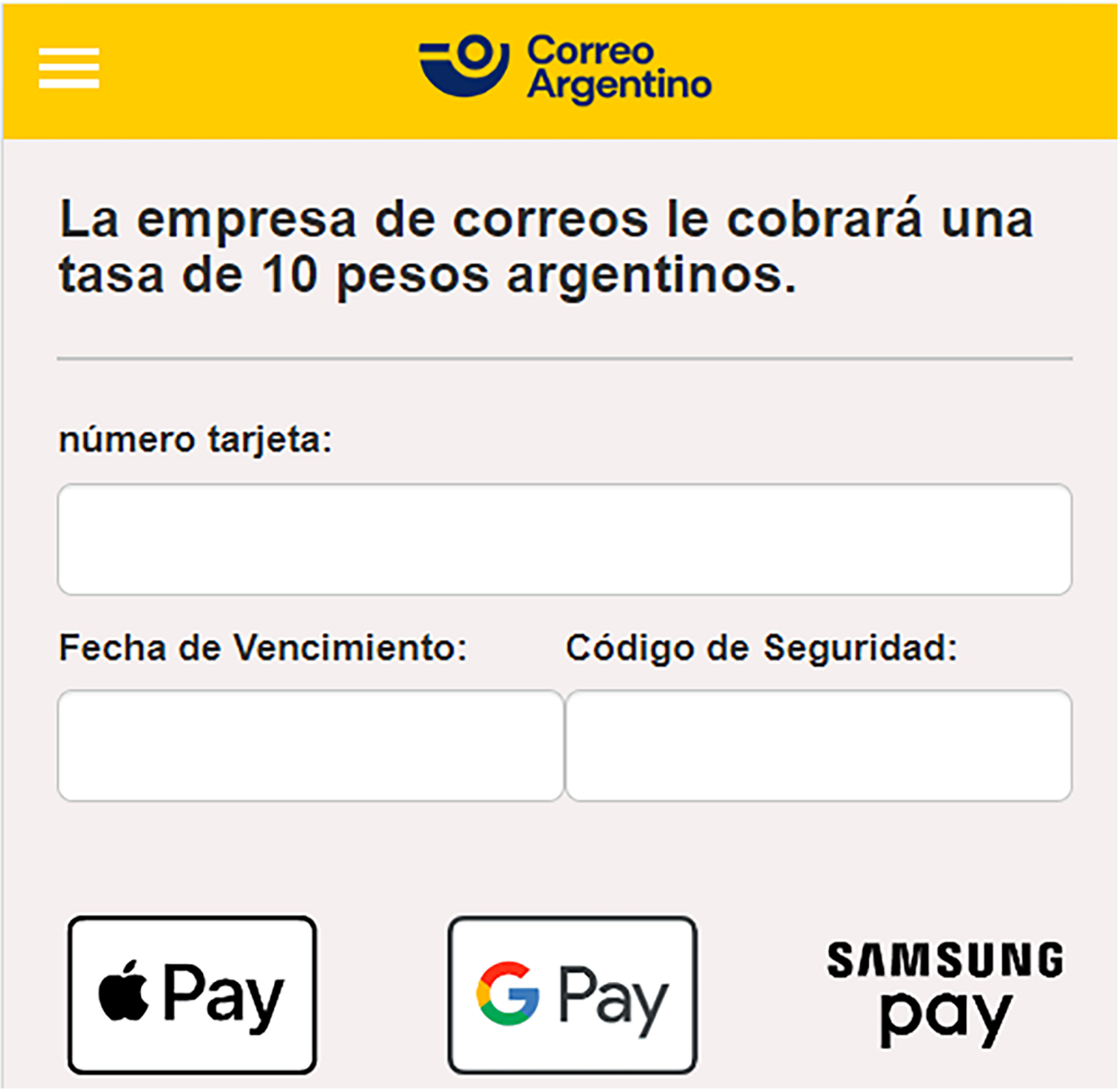
Municipios*

Código Postal*

Siguiente paso

En el siguiente paso, indicó el usuario, la página falsa solicita el pago de $10 para completar el trámite. “No es importante si te cobran o no esos 10 pesos. Lo que quieren es quedarse con los datos de tu tarjeta de crédito”, explicó Oliver Galak.

Efectivamente, el sitio solicita el número de tarjeta, la fecha de vencimiento y el código de seguridad.



En diálogo con **Infobae**, Galak aclaró que no realizó una denuncia formal, pero sí denunció el link como “*pishing*” en Google. “Vi que un usuario de Twitter con conocimientos de web hosting, que vio mi tuit, hizo la denuncia con el proveedor

del hosting. Además, la cuenta oficial de Correo Argentino me retuiteó y añadió un flyer con advertencias basado en mi denuncia, con lo cual evidentemente tomaron nota", comentó.

"Cientos de tuiteros me respondieron que recibieron mensajes similares. Me llegaron respuestas de usuarios que les pasó lo mismo en **España**, **México, Colombia, Uruguay, Australia, Chile, Venezuela, EEUU, Croacia, Israel, Costa Rica**,entre otros países", señaló.

También por mail

Asimismo, otros usuarios reportaron que recibieron un mail, también a nombre de "Correo Argentino", con información sobre una supuesta encomienda.

"Su encomienda procedente del exterior está bajo nuestra custodia en el centro de distribución logístico. Antes de entregarla, es necesario cumplir con los requisitos aduaneros. Para agilizar el proceso de liberación, requerimos el pago arancelario de $52.040,12. Por favor, adjunte una imagen legible de su DNI (frente y reverso) para gestionar el trámite aduanero", indica el correo.

"Una vez recibida la información, coordinaremos la entrega en su domicilio o en una de nuestras sucursales. Tenga en cuenta que el plazo para el pago es de 72hs. Agradecemos su cooperación y estamos a su disposición para cualquier consulta adicional", agregan en el mail.

En ese caso, la dirección falsa es "correoargentino-com-ar-id-" más una serie aleatoria de números y letras. En caso de responder con la imagen del DNI, los ciber delincuentes continúan con la estafa, solicitando los datos de la tarjeta de crédito.

Fuente: Infobae