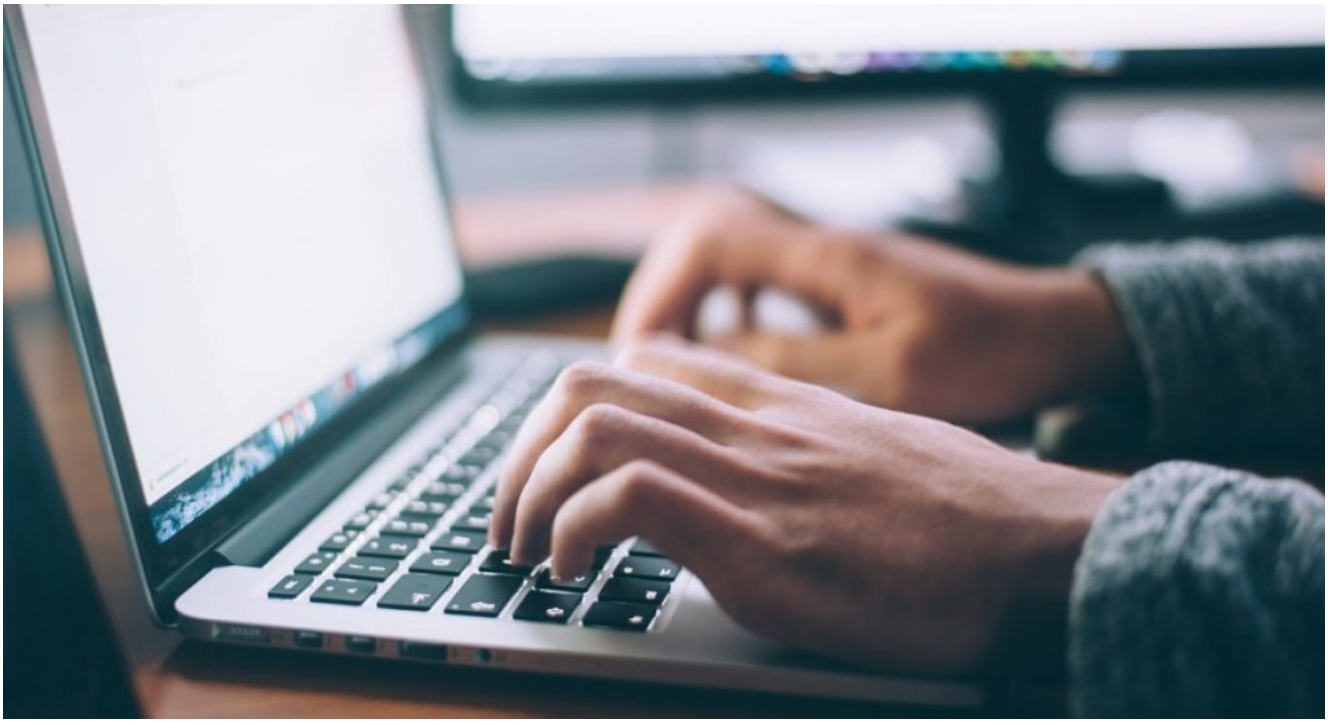
Una vieja estafa volvió a ser popular entre los ciberdelincuentes: conocé de qué se trata para evitar caer en el engaño

23/05/2024



Las estafas virtuales y el robo de datos son problemas cada vez más comunes en el mundo digital. En este sentido, el phishing (hacerse pasar por entidades confiables para engañar a las personas y obtener información confidencial) es cada vez más popular.

Así, una vieja estafa que utiliza esta técnica de **ciberdelincuencia**, volvió a reflotarse con el objetivo de obtener **información confidencial de las víctimas**, como nombres de usuario, contraseñas, números de tarjetas de crédito y otros datos sensibles.

En esta ocasión, se hizo cada vez más usual el procedimiento

en el que **los estafadores utilizan el nombre y la imagen del Correo Argentino para robar datos** personales y bancarios de los usuarios.

A través de **mensajes de texto (SMS) fraudulentos**, ciberdelincuentes envían un **enlace a una página web falsa** que imita la página oficial del organismo, donde la víctima debe ingresar su DNI y números de su tarjeta de crédito para liberar una supuesta entrega de un paquete a su nombre.

 ***Los delincuentes se hacen pasar por el Correo Argentino. Foto: NA***

Los delincuentes envían un mensaje en el que se lee que «**el paquete llegó al almacén, pero no pudo ser entregado debido a información de dirección incompleta**. Por favor, confirmá tu dirección en el enlace», adjuntando un link en el que los remitentes no deben ingresar para preservar sus datos personales.

Al entrar al sitio web que aparenta ser el oficial del Correo Argentino, el usuario en realidad ingresa en una página falsa, donde **se le solicita que introduzca su número de DNI, dirección de correo electrónico, número de teléfono y datos de la tarjeta de débito o crédito** para realizar un pago de 76.32 pesos argentinos y, así, liberar el supuesto paquete a su nombre.

Qué hacer si sospechás de un correo electrónico o mensaje

Evitar ser víctima de phishing requiere **estar alerta y tomar medidas preventivas** para proteger tu información personal y financiera:

about:blank

- **No ingresar en enlaces ni descargar archivos adjuntos** si son enviados de alguien que no tenés agendado.
- **Verificar directamente con la fuente**: es recomendable contactar a la organización directamente utilizando un número de teléfono o una dirección de correo electrónico obtenida de su sitio web oficial.
- **Reportar el phishing**: denunciar los correos electrónicos sospechosos a la organización afectada y a tu proveedor de correo electrónico. Muchas empresas tienen direcciones de correo electrónico dedicadas para reportar fraudes.
- **Eliminar el mail o mensaje**: después de reportarlo, elimina el correo electrónico o SMS de tu bandeja de entrada para evitar cometer errores.

Por último, en caso de ya haber sido víctima de la estafa, es necesario **dar de baja las tarjetas de crédito o débito y cambiar las contraseñas de tus cuentas bancarias**.

Fuente: Canal 26