

El Rancagüino / Jueves 29 de Mayo de 2025

Alertan de estafas en correos de Microsoft que introducen números de teléfono falsos para acceder a datos bancarios

Kaspersky ha alertado sobre un método de fraude con el que estafadores introducen números de teléfonos falsos en los correos electrónicos legítimos de Microsoft enviados a suscriptores empresariales, que funcionan como una trampa para que los usuarios llamen y puedan acceder a sus datos bancarios. Estos estafadores modifican el apartado de facturación en correos donde se informa de un supuesto cobro por una suscripción empresarial a Aplicaciones de Microsoft 365 para Empresas, con una gran número de servicios que no ha pedido el usuario, y sustituyen el nombre de la empresa y la dirección de facturación por un número de teléfono y un mensaje que anima a llamar a Microsoft si se necesita ayuda, según ha publicado la empresa multinacional rusa.

Al no poder responder a este



tipo de correos porque provienen de la dirección 'noreply' de Microsoft (una dirección que no admite respuestas), la única forma de contactar con la empresa tecnológica para pedir información acerca de ese cobro es llamando al número falso que adjuntan.

En este momento, si el receptor del correo decide llamar, los estafadores instan a la persona a

instalar un software de soporte y le envían un archivo EXE, según ha compartido un usuario en la red social Reddit. A continuación, una vez instalado el software, a este usuario le pidieron que accediese a su cuenta de banco para comprobar que se le había hecho la devolución, por lo que Kaspersky apunta a que el archivo instalado contendría alguna especie



de troyano de acceso remoto, con el que acceder a las credenciales bancarias de la víctima.

El método que emplearon los estafadores para modificar esos correos legítimos de Microsoft, de direcciones auténticas de la compañía se desconoce, aunque otro usuario de Reddit señaló que los estafadores podrían haber enviado estos correos falsos gracias al robo de "credenciales o versiones de prueba para acceder a Microsoft 365".

Otra teoría sugerida por Kaspersky apunta a que los estafadores podrían haber obtenido acceso a una cuenta con una suscripción activa a Microsoft 365 y utilizan la función de 'reenvío de facturación'. 