La estafa que preocupa a las autoridades: así toman el control de cuentas de homebanking

11/05/2023

La **Unidad Fiscal Especializada en Cibercrimen** (UFECI) lanzó una nueva advertencia a raíz de una **maniobra de phishing** (sustracción de datos personales mediante engaño) dirigida a **tomar el control de cuentas de homebanking** del **Nuevo Banco del Chaco**.

La advertencia tiene su origen en **una serie de denuncias formuladas ante esa unidad fiscal** por personas que recibieron en sus correos electrónicos diferentes mensajes con el logo y los colores del banco en los que **les solicitan que ingresen a un enlace provisto en el mismo correo** donde deben consignar su usuario y contraseña en un entorno similar al verdadero con el que operan los clientes de la entidad.

Según publicó el **Ministerio Público Fiscal de la Nación**, allí es donde se concreta la **sustracción de datos personales**, pues una vez que el cliente consigna sus credenciales (usuario y contraseña), las personas ocultas detrás del falso mensaje pueden acceder a las cuentas bancarias y tomar su control para realizar operaciones.

El mensaje engañoso funda la petición de las credenciales del cliente justamente en motivos de seguridad, con diferentes variantes, pero en todas se comunica en nombre del banco para informarle que su cuenta solicita verificación de identidad o que debido a varios intentos fallidos de inicio de sesión se bloquearon preventivamente sus credenciales para realizar la falsa validación de datos requerida.

«Después de varios intentos de ponernos en contacto con usted, **hemos tomado la decisión de enviarle este correo electrónico para informarle que su cuenta Nuevo Banco Del Chaco S.A. solicita verificación de identidad**, de no verificar procederemos a bloquear el acceso temporalmente. Completa esta verificación te tomará sólo unos minutos. Es por tu seguridad por eso procede a verificar tu cuenta y sigue disfrutando de nuestros servicios. Por favor, visite el siguiente sitio de confirmación», dice uno de los mensajes.

Otro de los mensajes con la dirección de correo electrónico del destinatario-víctima y lo torna próximo y verosímil, indica: «**Hola te informamos que debido a continuidad de intentos fallidos de inicio de sesión a tu cuenta, tus credenciales fueron bloqueadas preventivamente por motivos de seguridad.** Es necesario que ingreses al siguiente enlace en el botón de redirección para desbloquear el acceso a tu cuenta. Atentamente Equipo de Seguridad Banco del Chaco.» (sic).

Desde la UFECI, remarcaron que este tipo de maniobras dirigidas a la sustracción de datos personales no son nuevas, y que por lo general, cambia la fachada utilizada para presentarse ante diferentes grupos de víctimas.

Y **esto se da especialmente desde el 2020, que se han generado diversas campañas de envíos de este tipo de correos a un gran número de destinatarios** a nombre de diferentes bancos o firmas comerciales, como billeteras digitales, cuentas de correo (que una vez ganadas son usadas para, a su vez, distribuir correos de este tipo) o servicios de streaming.

También desde la UFECI **recomiendan verificar siempre la dirección de correo del remitente** y, si no es la oficial del banco, asumir que es falso.

Ante la duda, **se sugiere contactarse con el banco o ingresar al homebanking sin seguir el enlace remitido en el correo** recibido ni buscar la URL utilizando buscadores. Por caso, una buena práctica es ingresar al homebanking desde la página oficial del banco.

La UFECI además **solicita que, quien advierta accesos no autorizados a su cuenta, dé aviso al banco y recurra a las autoridades** locales para concretar su denuncia. En la Ciudad de Buenos Aires pueden realizarse denuncias de este tenor en el servicio telefónico de emergencias 911.

NA