CIBERCONSEJOS

PHISHING
SMISHING
VISHING

¡CONOCE LAS DIFERENCIAS!

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Phishing: la amenaza más común

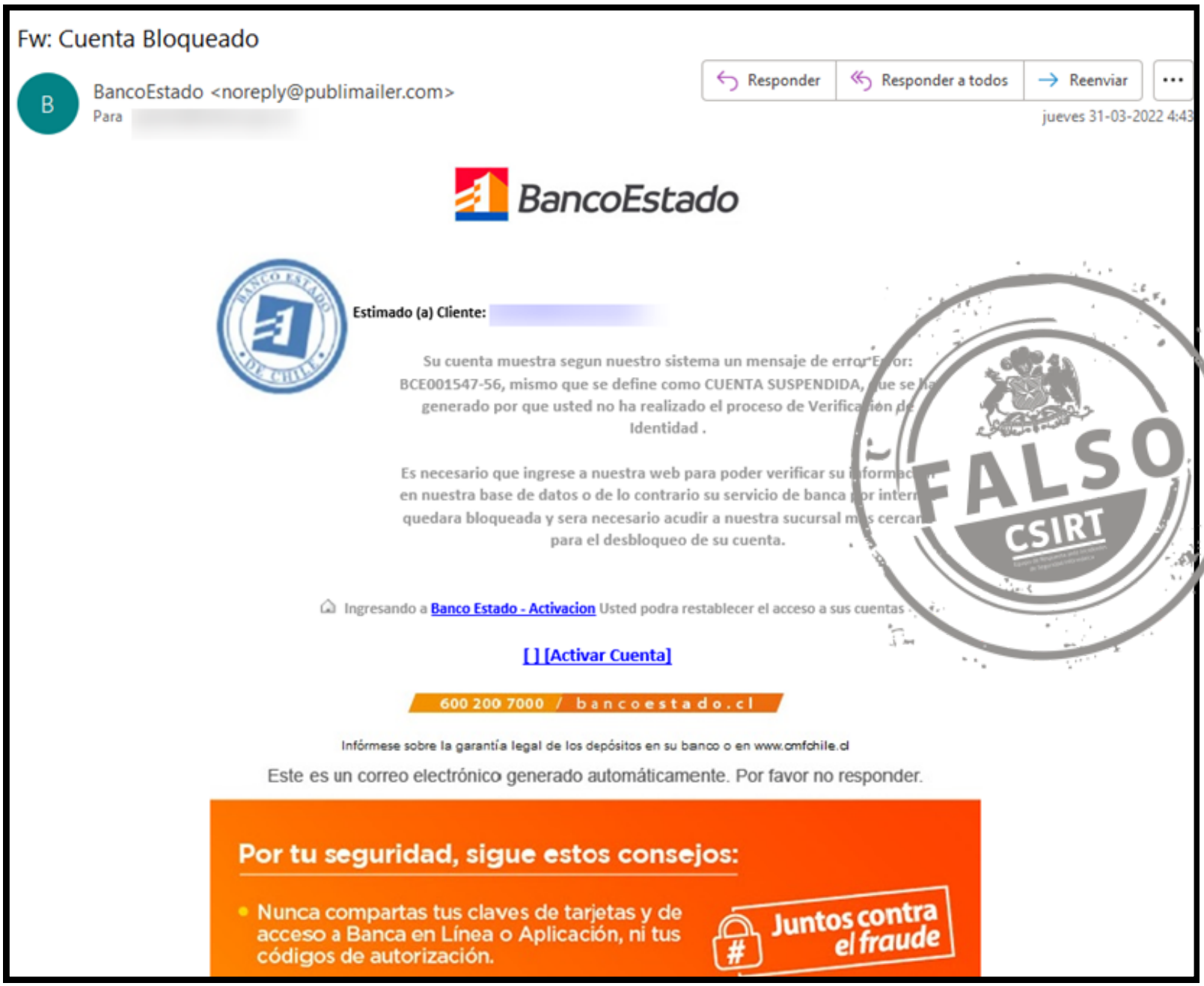
Es las forma más usada por los ciberdelincuentes para engañar a las personas. Consiste en intentar convencer al destinatario de un mensaje de descargar un malware, hacer clic en un link malicioso, o entregar al remitente información confidencial, como datos bancarios, de la persona o su empresa.

Para lograrlo, los delincuentes se hacen pasar por personas o instituciones de confianza para el receptor del mensaje.

Nunca respondas o hagas clic en enlaces no solicitados, especialmente si emplean mensajes alarmantes. Fíjate en el remitente y si tienes dudas, llama directamente a la persona o institución.

Un ejemplo de phishing

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



Smishing: phishing en SMS y mensajería

Se envían mensajes fraudulentos de texto (SMS) o por apps de mensajería que parecen provenir de fuentes legítimas, como bancos o empresas, solicitando información confidencial o haciendo que la víctima haga clic en enlaces maliciosos.

Un ejemplo de smishing

Corre0sChile: Por favor actualice su informacion de direccion dentro de 24 horas o perderemos su articulo: qrco.de/bepws8

FALSO CSIRT

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Vishing: phishing por voz

Su nombre es una combinación entre voz y phishing. Constituye una variante del phishing en la cual los delincuentes utilizan llamadas telefónicas (o de voz, en apps de ese tipo) para engañar a sus víctimas.

Para ello, se hacen pasar por representantes de instituciones financieras u otras entidades legítimas, con el objetivo de obtener información personal o financiera por teléfono.

Puede combinarse con el envío de mensajes, por ejemplo, para lograr un clic en un sitio malicioso