

CIBERCONSEJOS

**PHISHING
SMISHING
VISHING**

**¡CONOCE LAS
DIFERENCIAS!**

LOGIN
PASSWORD



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Phishing: la amenaza más común

Es la 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.



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática


Un ejemplo de phishing


Fw: Cuenta Bloqueado

BancoEstado <noreply@publemailer.com>
Para [Redacted]

Responder Responder a todos Reenviar

jueves 31-03-2022 4:43

 **BancoEstado**

 Estimado (a) Cliente: [Redacted]

Su cuenta muestra según nuestro sistema un mensaje de error "Error: BCE001547-56, mismo que se define como CUENTA SUSPENDIDA, que se ha generado por que usted no ha realizado el proceso de Verificación de Identidad .

Es necesario que ingrese a nuestra web para poder verificar su información en nuestra base de datos o de lo contrario su servicio de banca por internet quedara bloqueada y sera necesario acudir a nuestra sucursal más cercana para el desbloqueo de su cuenta.

Ingresando a [Banco Estado - Activación](#) Usted podra restablecer el acceso a sus cuentas.

[\[\] \[Activar Cuenta\]](#)


600 200 7000 / [bancoestado.cl](#)


Infórmese sobre la garantía legal de los depósitos en su banco o en [www.cmfchile.cl](#)

Este es un correo electrónico generado automáticamente. Por favor no responder.

Por tu seguridad, sigue estos consejos:

- Nunca compartas tus claves de tarjetas y de acceso a Banca en Línea o Aplicación, ni tus códigos de autorización.

 **Juntos contra el fraude**



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





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

