SUPERINTENDENCIA DE BANCOS

La Superintendencia de Bancos (SB), advierte al público en general:

Nuevas campañas de phishing ingeniería social vía correo electrónico, redes sociales y SMS/MMS que utilizan el COVID-19 y otros temas como excusa para el ataque.

SUPERINTENDENCIA DE BANCOS

«El phishing es una técnica utilizada por los ciberdelincuentes para engañarte y obtener información personal de los usuarios»

Los medios por donde actúan estos ciberdelicuentes son: mensajes de texto, mensajes por WhatsApp, por redes sociales o correos electrónicos

El objetivo es suplantar la identidad de organismos legítimos como Bancos, una red social o una entidad pública, para engañarnos y conseguir que revelemos información personal como contraseñas, número de teléfonos y códigos de billeteras de dinero electrónico, números de la tarjeta de crédito, cuentas bancarias, etc.

¿QUÉ TIPO DE INFORMACIÓN ROBA?

Datos personales

- Direcciones de correo
- Número de documento de identidad
- Datos de localización y contacto

Información financiera

- Número de tarjetas de crédito
- Números de cuentas
- Información de Home Banking o e-commerce

Credenciales de acceso

- Redes Sociales
- Cuentas de correo

PRINCIPALES MEDIOS DE PROPAGACIÓN

- Correo electrónico
- Redes Sociales
- SMS/MMS
- Llamados telefónicos
- Infección de malware

CIRCUITO DE UN ATAQUE

1 Falsificación de un ente de confianza

2 Envío de mensajes por algún medio de propagación

3 Un porcentaje de usuarios confía en el mensaje y hace clic

4 Los usuarios acceden a un sitio web falso e ingresan sus datos personales

Consecuencias:

- Robo del dinero en la cuenta bancaria
- Uso indebido de la tarjeta de crédito
- Estafa
- Venta de los datos personales
- Suplantación de identidad
- Envío de publicidad

5 El atacante obtiene los datos y los utiliza con fines maliciosos

La SB recomienda para evitar el phishing:

Evita dar tus datos como norma general.

Desconfía de la escritura incorrecta. Ten en cuenta que una entidad seria, como puede ser tu banco o la administración pública, nunca cometerían errores gramaticales.

Desconfía de la urgencia. Otra de las técnicas utilizadas por estos ciberdelincuentes es la de pedir acciones en un periodo muy corto de tiempo.

Nunca entrar en la web del banco pulsando en links incluidos en correos electrónicos. No hacer clic en hipervínculos o enlaces que vengan adjuntos en el correo.

Introducir datos confidenciales únicamente en webs seguras. Las webs seguras comienzan por “https://” y deben aparecer en el navegador el icono de un pequeño candado cerrado.

Revisar periódicamente las cuentas. Esto, para estar al tanto de cualquier irregularidad en sus transacciones online.

La mejor forma de acertar es siempre rechazar de forma sistemática cualquier correo electrónico o comunicado. Elimina este tipo de correos.

Ninguna Entidad pide tu contraseña. Tu banco no te va a pedir nunca tu número de cuenta ni clave de acceso, tu red social favorita tampoco te va a solicitar tu contraseña de acceso.

SUPERINTENDENCIA DE BANCOS

Si sospecha que a sido victima de algún tipo de ataque:

Ponerse en contacto rápidamente con su Entidad.

El Banco Central del Paraguay (BCP) habilitó una oficina de Defensa del Consumidor Financiero con el objetivo de garantizar la información y la seguridad de los usuarios de servicios financieros. Se habilitó el correo electrónico usuariofinanciero@bcp.gov.py, para la recepción de reclamos o consultas.