Oficio Nro. SEPS-SGD-IGT-2021-25968-OFC

Quito, D.M., 12 de octubre de 2021

Asunto: Recomendaciones para el manejo de información y administración de ciberseguridad en el Sector Financiero Popular y Solidario

Señores Gerentes
ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

De mi consideración:

Como alcance al oficio SEPS-SGD-IGT-2021-21112-OFC y ante el crecimiento de la oferta de servicios financieros electrónicos y el aumento de los delitos informáticos enfocados a los socios y clientes de estos es el de Phishing término por el que se conoce a un tipo de fraude cuyo objetivo es el de pescar (fish) mediante **ingeniería social y/o** *malware* información confidencial, como números de tarjetas de crédito, claves de acceso, datos de cuentas en entidades financieras u otros datos personales de las víctimas, **suplantando en ellos la identidad de su legítimo titular**

Existen distintas versiones de esta estafa, pero el modus operandi suele seguir los mismos patrones. Los estafadores utilizan tácticas alarmistas o solicitudes urgentes para que los usuarios se vean obligados a proporcionar la información solicitada. Una de las formas de llevar a cabo esta técnica es mediante una llamada telefónica o SMS donde los estafadores se hacen pasar por una entidad financiera o cualquier empresa de confianza para advertirle que necesitan algunos datos confidenciales con cualquier excusa que pueda convencer a la víctima. Pero la forma más usada es mediante el correo electrónico.

Los mensajes de correo electrónico de phising tienen diversas formas:

· Puede simular que viene de una entidad financiera, de una empresa conocida o incluso de las redes sociales.

· El correo electrónico puede simular que proviene de un contacto de su libreta de direcciones de correo electrónico.

· Pueden solicitarle que realice una llamada telefónica. Al realizar la llamada una persona o una unidad de respuesta de audio esperan para conseguir tu número de cuenta, tu número de identificación personal, tu contraseña u otros datos personales valiosos.

· Pueden incluir logotipos de apariencia oficial y otra información tomada directamente de sitios web legítimos, y pueden incluir detalles convincentes acerca

de tu historial personal. Los estafadores obtienen esta información de las redes sociales.

· Pueden incluir vínculos a páginas falsificadas en los que se le solicita facilitar información personal

Ante la presencia inminente de este riesgo presentamos algunas recomendaciones que deben socializarse con sus funcionarios, proveedores, socios y clientes para prevenir la materialización de estos eventos.

- Evitar el uso de correo electrónico, menajes de texto, llamadas telefónicas o redes sociales para el envío de información personal o financiera
- No abrir correos electrónicos ni enlaces de remitentes que no sean de contactos conocidos, es mejor eliminarlos
- Comprobar siempre se acceda a sitios seguros verificando que el URL de la página inicie con “https”
- Usar siempre antivirus y mantenerlo actualizado y con licencia en cualquier dispositivo que acceda a internet.
- No acceder a las páginas de internet a través de enlaces en correos otras páginas o portales, sino escribiendo el URL en la barra de direcciones.

Entre otras recomendaciones pueden realizar son:

- Monitoreo de Redes Sociales y dominios institucionales
- Monitoreo de campañas de phishing externas
- Combatir la falsificación de correos (D-MARC)
- Sensibilizar a funcionarios, proveedores, socios y clientes sobre diferenciar comunicaciones fraudulentas y legítimas.
- Establecer procesos antiphishing.

Atentamente,

Firmado electrónicamente por:
Jorge Andrés Moncayo Lara
INTENDENTE GENERAL TÉCNICO
2021-10-12 15:24:14

Jorge Andrés Moncayo Lara
INTENDENTE GENERAL TÉCNICO