INTERCAM Banco

Estimado Cliente.

En Intercam tu seguridad es lo más importante y en esta ocasión quisiéramos informarte sobre una modalidad de fraude que está en aumento: FRAUDE BEC (Business E-mail Compromise) o Suplantación de Identidad por correo electrónico.

Es un tipo de estafa dirigida a empresas que realizan transferencias electrónicas. **Consiste en engañar a un empleado, principalmente de áreas financieras o tesorería, dentro de la empresa, para que ejecute transferencias de fondos a la supuesta cuenta de un proveedor o socio (utilizando nombres conocidos),** cuando en realidad termina en la cuenta bancaria del atacante. **Las modalidades más usuales son:**

1. **Fraude CEO:** el defraudador envía un correo electrónico que parece proceder del CEO o de algún directivo de la empresa a un empleado que tenga capacidad para realizar transferencias, dándole instrucciones para que envíe fondos a una cuenta que en realidad fue aperturada por el defraudador
2. **Orden de pago falsa:** el defraudador, tras comprometer la cuenta de un usuario, busca en el correo electrónico una orden de pago que venza pronto (revisan historial), para después contactar al área de Finanzas y pedirles que cambien la cuenta de pago por una diferente. (No cambia beneficiario, solo cambian Banco y número de cuenta)
3. **Hackeo a correos de proveedores:** el defraudador compromete la cuenta de correo electrónico del proveedor, por lo que el Cliente recibe instrucciones de cambio de pago utilizando el mismo método de orden de pago falsa, utilizan facturas, cartas o cualquier documento que encuentran disponible para hacer más real la conversación vía correo electrónico

Independientemente de la modalidad, siempre hay una primera etapa de reconocimiento en la que los defraudadores recolectan y analizan información sobre la entidad y personas en roles específicos, relacionadas con el proceso de pagos y transferencias. Para ello, emplean diversas técnicas de compromiso para acceder a información clave.

¿Cómo puedes protegerte?

Correos electrónicos:

- Confirma siempre vía telefónica con tus proveedores o Clientes las instrucciones de pago recibidas (número de cuenta, beneficiarios)
- Verifica el dominio de los mails recibidos, previo a ejecutar alguna solicitud de pago, la variación puede ser mínima
- Desconfía cuando mencionen en el correo que solo estarán disponibles por el mismo correo electrónico
- Presta atención a la forma de expresarse de la persona que escribe, suele ser diferente a la de la persona real
- Elimina cualquier mensaje de origen sospechoso o que solicite información personal o financiera
- No ingreses contraseñas, des clic a enlaces o abras documentos adjuntos

Contraseñas:

- Utiliza claves que no se relacionen con datos personales como fechas de nacimiento, números telefónicos o nombres de familiares; utiliza letras mayúsculas, minúsculas, números y símbolos
- Nunca envíes tus claves por correo electrónico ni las compartas con otros

Computadoras Seguras:

- Evita equipos públicos para realizar movimientos bancarios o para ingresar a tus cuentas de correos. Tu información puede quedar grabada en ellos con el uso de software maligno
- Mantén parches de seguridad y software antivirus actualizados para tu computadora, tus navegadores de internet y dispositivos móviles
- No descargues automáticamente ningún archivo adjunto; asegúrate de desactivar esta función en tu dispositivo móvil

#HumanismoFinanciero

Centro de Atención a Clientes Intercam

Desde cualquier parte de México: 55 5033 3333 | Desde EE.UU. y Canadá: 1 844 859 9078 | Desde cualquier parte del mundo: +52 55 5033 3333