Departamento de TIC

Capsula informativa

Campaña de Phishing y Smishing (Mensajes enviados por SMS).

Buenas tardes, hoy en la Capsula Informativa. Les queremos recordar que empezamos este año con muchos ataques dirigidos a buscar información sobre nosotros. Ya en una capsula anterior se explicó que era el Phishing: es un método para engañarle y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica.

Hoy en día se están haciendo mas comunes estos tipos de ataque, como por ejemplo hoy llego a un correo del IDIAF este mensaje:

Asunto: RE: Departamento de TI 🔔 🔔 🔔
Fecha: Tue, 20 Feb 2024 13:38:05 +0000
De: Cheryl Quiroz <cheryl.quiroz@minsal.cl>
Para: Cheryl Quiroz <cheryl.quiroz@minsal.cl>

Administrador de sistema
Su contraseña caducará en unos días. (Haga clic en Mesa de ayuda) para actualizar su contraseña actual y cambiar automáticamente al correo electrónico más reciente de Outlook Web Apps 2024.

Si su contraseña no se actualiza hoy, su cuenta se cerrará en 12 horas.
administrador de sistema,
conectado a Microsoft Exchange.
© 2024 Todos los derechos reservados Microsoft Corporation.

Por favor, tengas cuidado con este tipo de correos, El Departamento de Tecnología no les va a pedir que actualicen nada, sin previo aviso (llamada telefónica o carta física). Pero de Igual forma, siempre que vean un correo solicitando información, lo mejor es comunicarse directamente con la entidad que emitió el correo. Pero NUNCA usar los números que vienen en el mismo correo. Si no, deben buscarlo en fuentes confiables.

OJO este tipo de correo no solo llega con cosas del trabajo, también pueden llegar haciéndose pasar por cualquier entidad Bancaria, tienda o negocio que posiblemente, sean cliente.

Que hacer: Solo, deben borrar el correo **sin intentar ver que es lo que están enviando** y reportarlo a su Encargado de tecnología de su Zona.

Gracias.