¡Estimados todos, buenas tardes!

Están llegando correos similares a este, los cuales son maliciosos,

Tips:

Lo que DEBES hacer ✅

* Revisa el remitente : Verifica que la dirección de correo coincida con el dominio oficial de la empresa (es una recomendación general, aunque en este caso puede engañarnos).

* Analiza el enlace sin hacer clic: Coloca el cursor sobre el link (sin presionarlo) para ver la URL real. Si no coincide con el sitio oficial, es falso.

* Desconfiar del sentido de urgencia : Los atacantes usan frases como "cuenta bloqueada" o "acción inmediata" para que actúes sin pensar.

* Reportar y bloquear : Utiliza las herramientas de tu cliente de correo para marcar el mensaje como "Phishing" o "Spam".

Lo que NO DEBES hacer ❌

* No hagas clic en enlaces : Nunca sigas links que provengan de correos que no solicitaste, especialmente si tienen errores ortográficos o dominios raros (.iceiy.com).

* No entregues datos personales : El IPN no te pedirá tu número de WhatsApp o contraseña a través de un correo electrónico.

* No respondas al mensaje : Contestar solo confirma a los atacantes que tu cuenta está activa y te enviarán más ataques en el futuro.

* No descargues archivos adjuntos : Aunque este correo no los tiene, muchos suelen incluir malware que se activa al abrir documentos o imágenes.

* No te dejes llevar por los logotipos : El uso de imágenes oficiales y logotipos como el de Microsoft es una táctica común para generar una falsa sensación de confianza.