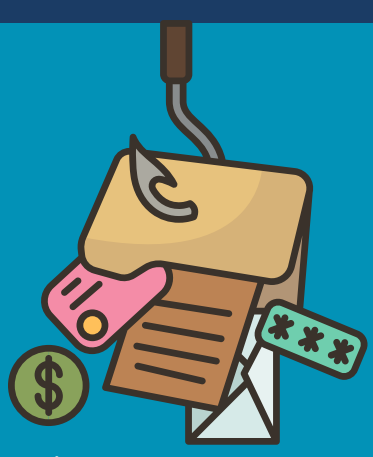
RECOMENDACIONES GENERALES DE CIBERSEGURIDAD

Conocelas

CUIDADO CON EL PHISHING Y SUS DERIVADOS!



Evío de correos electrónicos (Phishing), mensajes de texto (Smishing) y llamadas o mensajes de voz (Vishing) fraudulentos que aparentan ser de proveniencia legitima para el robo de datos bancarios y personales.

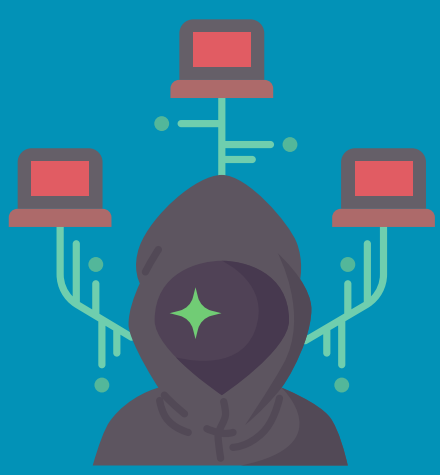
- Un correo phishing, mensaje de voz, o de texto típicamente contiene comentarios escandalosos
- Leer cuidadosamente el contenido del mensaje, analizar si este es sospechoso o pide entrar a links o dar informacion confidencial

NO ACEPTES NUEVAS PERSONAS EN NINGUNA RED SOCIAL PERSONAL

Si lo haces, verifica que conoces a esta persona y si parece ser un perfil real con contactos, si te es sospechoso no aceptes ninguna notificación y bloquea el contacto de inmediato

NO ABRAS NINGÚN LINK, ARCHIVO O FOTOS DE NINGUNA FUENTE QUE NO SEA DE UN MIEMBRO OFICIAL DE LA CAMPAÑA

Esto podria ser un intento de ataque con virus o robo de datos confidenciales



UTILIZA MEDIOS SEGUROS PARA COMUNICARSE

Utiliza Threema work para la comunicación de temas confidenciales, en caso de no usar threema las conversaciones pueden ser hackeadas e interceptadas

EN CASO DE QUE PIENSES HABER O QUERER SER ATACADO, CONTACTA AL EQUIPO DE CIBERSEGURIDAD

Puedes contactarnos mediante Threema Work