FINAGRO 30 AÑOS

¿Qué es *smishing* y vishing?

¡RECUERDA! Los ciberdelincuentes están aprovechando la emergencia sanitaria para lograr engañar y cumplir sus objetivos de estafa o robo de datos, en estos momentos para llegar a sus víctimas han aprovechado las **fake news, ayudas del gobierno, alivios de entidades bancarias** y están usando mucho los mensajes y llamadas falsas, ciberataques conocidos como:

Smishing

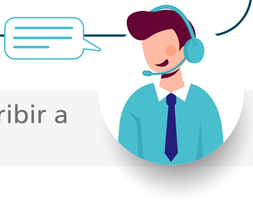
Ataque cibernético que usa como canal los **mensajes de texto** a celulares, por medio de los cuales busca **engañar** a la víctima para estafarla. Por ejemplo, el atacante envía un mensaje de texto (SMS) para informar de supuestos premios, ayudas, subsidios etc.; el atacante solicita una consignación o recarga de minutos para hacer efectiva la entrega del supuesto premio o ayuda engañando de esta forma a la víctima.

Vishing

Ataque cibernético realizado por medio de **llamadas**, estos ataques suplantan la voz automática de las entidades bancarias o simplemente el atacante llama y por medio de engaños se hace pasar por un funcionario de alguna entidad para obtener información personal de la víctima. Las Entidades bancarias JAMÁS pedirán sus datos de acceso, números de tarjeta, etc.

¿Qué tienen en común?
Estos ataques se realizan por medio de un método conocido como **ingeniería social,** lo cual quiere decir que por medio de engaños busca hacerse con información de la víctima suplantando entidades o personas de confianza.

¿Qué debes hacer?
Siempre **desconfía** de los mensajes o llamadas por medio de los cuales se solicite confirmar tu usuario y contraseña, información personal o bancaria en general; si tienes dudas no brindes información y ponte en contacto de inmediato con la entidad de donde se supone te han contactado.



Si tienes alguna inquietud puedes escribir a
jguatame@finagro.com.co

Gerencia de Riesgos