FINAGRO 30 AÑOS

Ingeniería social = engaño

¿Qué es?

La **ingeniería social** es un método por el cual un ciberatacante busca **engañar a sus víctimas** para que **accedan a links, sitios web, conteste preguntas o envíe información** para proceder a estafar, suplantar o vender los datos obtenidos en internet.

"Durante la pandemia los **delitos informáticos se han incrementado en 59%** y la suplantación de los sitios web en **364%**. Cifra que solo muestra los casos que se han denunciado ante las autoridades, ya que **hay miles de personas que no denuncian** porque creen que es normal, no saben que es un delito, o se resignan". **Fuente:** La República.

Debes identificar las siguientes modalidades de engaño

Enlaces o links falsos. Estos provienen de un usuario no conocido o un usuario suplantado. Estos links no solo llegan por correos electrónicos, sino también por redes sociales, mensajes de texto o chat como WhatsApp.

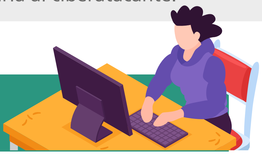
Phishing. El cuál es un ciberataque que intenta suplantar generalmente entidades bancarias para que la víctima acceda a un sitio web o un enlace y solicita sus datos de acceso.

Vishing. Ciberataque que se realiza por medio de llamadas y *Smishing* cibertaque que se realiza por medio de mensajes. Los dos tienen en común: el intento del ciberatacante por engañar haciéndose pasar por empleado de una entidad e intenta obtener información como **usuarios**, **contraseñas**, **números de tarjeta**, **dirección**, sobre la **familia** etc.

Baiting. El cuál es un ciberataque que consiste en dejar un dispositivo de almacenamiento **(USB) "olvidado"**, la víctima lo recoge y al conectarlo a su equipo se instalan archivos maliciosos que pueden capturar su información para enviarla al ciberatacante.

¿Qué hacer?

Sigue las siguientes recomendaciones



- → **Haz caso a tu intuición**, si no te produce confianza mejor no abras un correo o link.
- → **Antes de acceder a un correo electrónico** revisa su procedencia, mira el remitente, si solicita acceder a links desconfía y más aún si piden datos de acceso como usuario y contraseña. Recuerda las entidades bancarias NO solicitan esta información.
- → **Si recibes mensajes** que buscan generar pánico o miedo como fotocomparendos, prueba de COVID-19, ayudas humanitarias etc. No hagas caso, si tienes duda al respecto recurre directamente a la entidad que supuestamente te envía el correo y haz directamente la validación con ellos.
- → **Debes ser cuidadoso** cuando te soliciten información en sitios web, no diligencies los formularios a la ligera y siempre verifica que la dirección del sitio web sea legítima. Ojalá que inicie con https, lee las políticas.
- → **No hagas caso de mensajes** que indiquen que ganaste la lotería, un carro o televisor, nada es gratis.
- → **Evita usar la misma contraseña** para todos tus servicios web, en lo posible activa el doble factor de autenticación (token) y cambia con frecuencia la contraseña.
- → **Mantén tu equipo de cómputo actualizado** y con un antivirus instalado al igual que en tu celular.
- → **Si has recibido mensajes sospechosos** o has sido víctima de un ciberataque denuncia, puedes hacerlo dirigiéndote al CAI Virtual de la Policía Nacional .

CAI VIRTUAL

Recuerda, que la ciberseguridad debe ser tu prioridad, tu información es importante y debes protegerla.

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

Gerencia de Riesgos