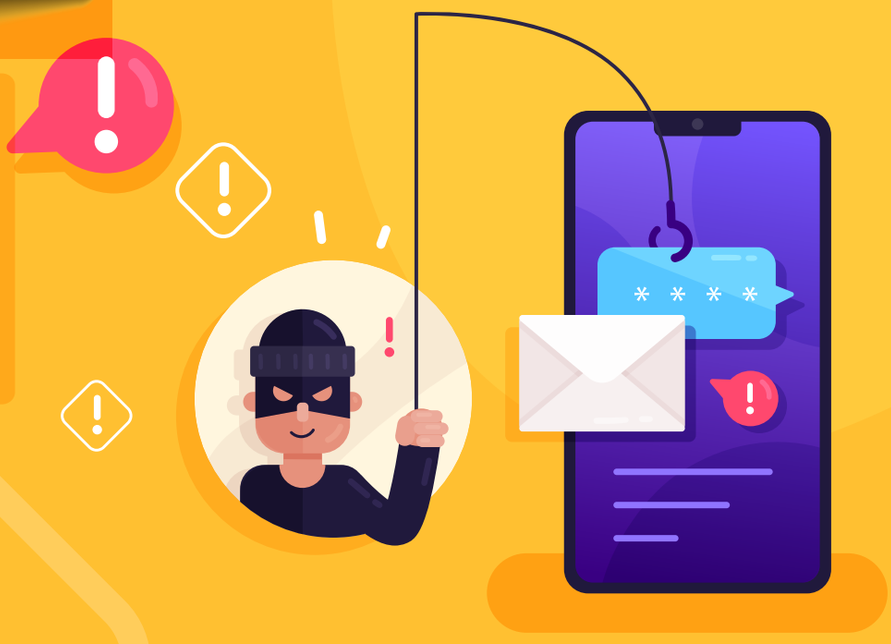
EDUCACIÓN FINANCIERA EN TU INSTITUCIÓN

¡CUÍDATE DEL SMISHING!

El Smishing es una nueva versión del fraude conocido como Phishing. Se realiza a través de teléfonos móviles y su objetivo principal es el robo de información personal y financiera de las personas.



TIPOS DE ATAQUES DE SMISHING

- **Verificación de cuenta:** La víctima recibe un mensaje de texto de una supuesta empresa o proveedor de servicios.
- **Premios o loterías:** Se informa a las víctimas que han ganado un premio, o la lotería.
- **Alertas de fraude bancario:** Los mensajes parecen proceder del banco de la víctima, advirtiendo transacciones no autorizadas o actividades sospechosas.
- **Estafas fiscales:** La persona recibe mensajes que dicen ser del SAT.
- **Cancelación de servicios:** La víctima recibe un mensaje de que una suscripción o servicio está a punto de cancelarse por un problema de pago.
- **Paquete fantasma:** Se recibe un mensaje informándole a la víctima que su paquete no pudo ser entregado y solicitan ingrese a un link.

¡PROTÉGETE!

- No hagas clic en enlaces sospechosos o en mensajes de texto.
- No reveles datos personales a través de SMS.
- Revisa tus cuentas bancarias regularmente.
- Instala un antivirus en tus dispositivos.
- Descarga aplicaciones solo de tiendas y desarrolladores oficiales.

Hacienda
Secretaría de Hacienda y Crédito Público

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS