

Conoce cómo se presentan y qué puedes hacer para protegerte.

01

## Fraudes digitales y en redes sociales



### Phishing

Son correos electrónicos que **parecen reales**, con logotipos y colores del banco, pero son **falsos**.

Te dicen que hay un problema con tu cuenta o que debes confirmar tu identidad.

Te piden que hagas clic en un **enlace peligroso** que lleva a una página falsa donde tú mismo **escribes tu usuario, NIP o token**.

### Redes sociales

En Facebook, WhatsApp o Instagram pueden aparecer **publicaciones con préstamos falsos, sorteos o beneficios “urgentes”**.

A veces se hacen pasar por el banco o incluso **clonan el perfil de una persona que conoces** para engañarte.

### Smishing

Es como el phishing, pero **por mensaje de texto**.

Te mandan un SMS diciendo que tu cuenta fue bloqueada o que tienes un cargo extraño.

Incluye un **enlace falso** que al abrirlo puede robar tu información o instalar un virus.

### Apps falsas

Hay aplicaciones que parecen reales pero no lo son.

Las apps falsas se descargan fuera de las tiendas oficiales (como Play Store, APPGallery o App Store).

Al instalarlas, **roban tus contraseñas o piden permisos para controlar tu celular**.

### Vishing

Te llaman haciéndose pasar por **empleados del banco**.

Te dicen que hubo un cargo raro o que debes actualizar tu información.

Te piden códigos, token, NIP o contraseñas, **pero en realidad quieren robarte**.

### Malware bancario

Es un virus que se instala en tu celular o computadora y **espía tus movimientos**.

Algún malware incluso **copian lo que escribes** y lo envían a los delincuentes.

02

## Fraudes por suplantación de identidad



### Correos de suplantación

- El delincuente se hace pasar por una empresa, una persona o el banco.
- Usa correos similares a los oficiales.
- Los correos pueden tener errores ortográficos, urgencia o promesas irreales.

### Solicitudes de créditos o compras sin autorización

Si tienen tus datos, pueden:

- Sacar un préstamo a tu nombre.
- Solicitar tarjetas.
- Comprar a crédito.
- Hacer compras en línea.



### Robo de datos personales

- Obtención de INE, RFC, CURP, comprobantes y datos bancarios para abrir cuentas o pedir créditos.
- No compartas documentos por internet; destruye físicamente los que deseches y monitorea tu reporte de crédito, ya sea en Buró de Crédito o en Círculo de Crédito.

### ¿Qué hacer si alguien se hace pasar por ti?

01 **Llama de inmediato al banco** y reporta lo sucedido.

02 Pide que **bloqueen movimientos**.

03 Presenta un reporte en CONDUSEF si es necesario.

04 Denuncia el caso ante el Ministerio Público (fiscalía digital).

05 Si tienes buró de crédito, pide una alerta de protección.

## Regla de oro

NO compartas tus datos personales, claves ni códigos.

Detente, piensa y verifica dos veces antes de actuar; si algo parece sospechoso, llama directamente a tu banco.

