



# Phishing

(Suplantación de identidad)

## ¿Qué es Phishing?

Es cuando alguien se hace pasar por una identidad conocida ya sea una red social conocida, banco, organismo, etc... con el fin de robarte información personal.

## ¿Qué buscan robar?

**Información financiera** como números de tarjeta de crédito y números de seguridad, claves de acceso a sitios bancarios.

**Nombre de usuarios** de cuentas de servicios como Netflix, Facebook u otra red social.

**Datos personales** como números de teléfono, dirección de correo, etc.

## ¿Cómo funciona?

Recibes en tu buzón de entrada un correo que suplanta la identidad de una empresa y **contiene un enlace a un sitio falso, o un archivo adjunto infectado** (ese archivo suele llegar en formato Word, Excel, pdf). Si ingresas al enlace se te pedirá realizar una acción como: completar un formulario con tus datos. Esa información es aprovechada para robar tu dinero o vender tus contraseñas.

## ¿Cómo protegerte?

- **Presta atención** a la dirección remitente del correo y a la forma en que está redactado.
- **Desconfía** de qué información te solicitan.
- **Recuerda** que ningún banco o plataforma digital te pedirá que modifiques tus datos personales a través del correo sin que tú lo hayas solicitado.



**En caso de haber caído en engaño, favor cambiar tus credenciales de acceso**

## Algunos ejemplos de Phishing que han ocurrido en los últimos meses:

