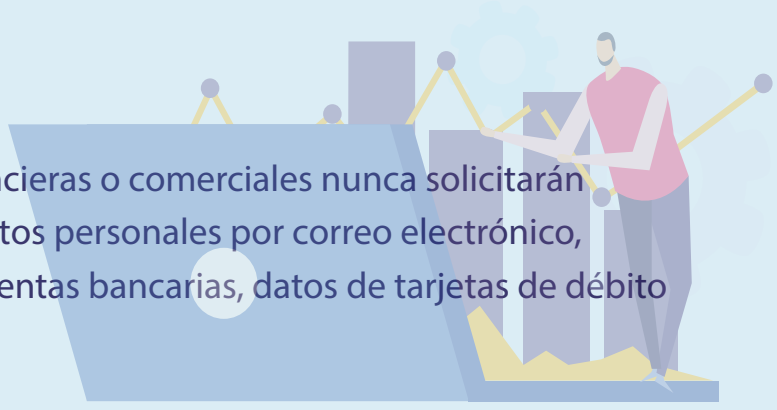
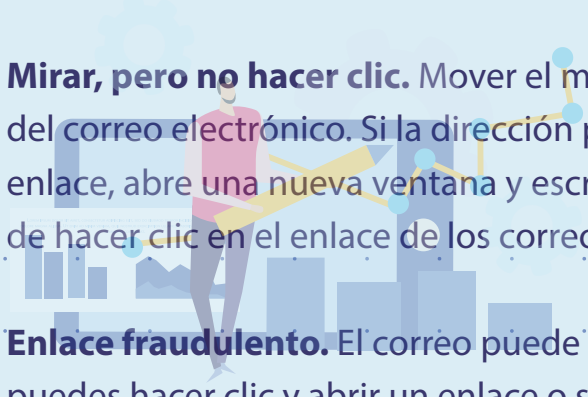
¿Cómo Identificar un Correo Phishing?



- **Información personal**. Las instituciones financieras o comerciales nunca solicitarán información confidencial, que consistan en datos personales por correo electrónico, incluyendo usuarios, contraseñas, datos de cuentas bancarias, datos de tarjetas de débito y crédito.

- **Estafa.** Ellos pretenden ser instituciones financieras o comerciales con quienes se mantiene relación y envían mensajes por la vía electrónica para hacer que revele su información personal.



- **Mirar, pero no hacer clic.** Mover el mouse sobre cualquier enlace incrustado en el cuerpo del correo electrónico. Si la dirección parece rara, no hagas clic en ella. Si deseas probar el enlace, abre una nueva ventana y escribe la dirección del sitio web directamente en lugar de hacer clic en el enlace de los correos electrónicos no solicitados.

Enlace fraudulento. El correo puede ser en su totalidad una imagen, sobre la cual puedes hacer clic y abrir un enlace o sitio fraudulento.

- **Destinatarios sin referencia.** En muchas ocasiones los mensajes no están dirigidos de manera personal, utilizan referencias como: cliente, usuario o términos similares.

- **Adjuntos.** Puede contener archivos adjuntos, que no deben ser descargados.

- **Duplicación.** Los ladrones toman los números de las tarjetas de crédito o débito utilizando un dispositivo de almacenamiento electrónico especial que registra la información cuando se procesa la tarjeta.

- **Vínculos acortados.** Especial precaución con los vínculos que en algunos casos no se relacionan a sitios seguros, utilizan protocolos no seguros como http:// al inicio de la dirección.

- **Crean incertidumbre.** Generan en el usuario la necesidad de dar una respuesta urgente, ingresando a los vínculos o descargando archivos. **Correos Maliciosos.** La firma del mensaje no muestra detalles de la empresa o contiene información limitada.