Banamex

Glosario para tu seguridad digital

Siempre seguro

Glosario

Malware

Así empezó la estafa...

Martha descargó una supuesta actualización de seguridad desde una página no segura. **Sin saberlo, instaló un malware que robó sus contraseñas y datos bancarios.**

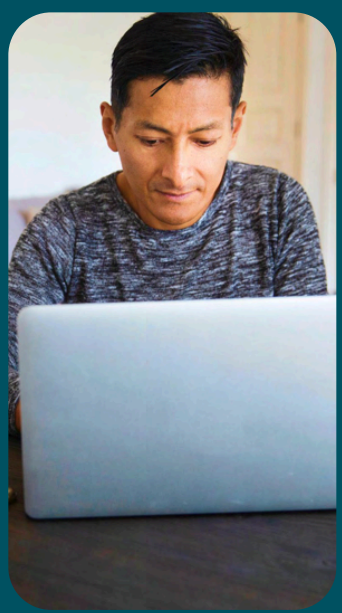
Consejo

- No descargues archivos o programas de fuentes no confiables.
- Mantén tus dispositivos y antivirus actualizados.
- Para aumentar tu protección, Banamex pone a tu disposición la herramienta IBM® Security Trusteer Rapport. Descárgala totalmente gratis en BancaNet®.

Phishing

Así empezó la estafa...

Juan recibió un correo de su "banco" **solicitando un cambio de contraseña por actividad sospechosa** en su cuenta. Sin dudarlo, **hizo clic en el enlace e ingresó sus datos. La página era falsa, y su cuenta fue comprometida.**



Consejo

Verifica siempre la autenticidad de los correos y páginas antes de ingresar tus datos.

Quishing

Así empezó la estafa...

Carla fue a comer a un restaurante y **escaneó el código QR que estaba en la mesa**. Además de enviarla al menú, **le descargó un código malicioso que tomó control de su dispositivo**, robando su información personal y datos bancarios.

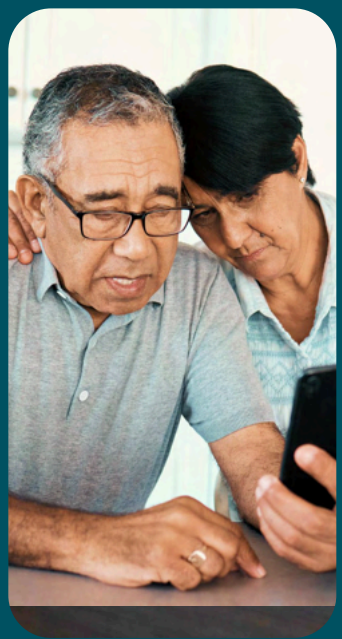
Consejo

- Evita escanear códigos QR en lugares públicos como restaurantes, parquímetros, estacionamientos o publicidad en la calle.
- Verifica siempre el link al que te van a direccionar.

Sim Swap

Así empezó la estafa...

Jorge recibió un SMS sospechoso, en el que le solicitaban información personal. Tras responder, su celular se quedó sin recepción y ya no pudo acceder a sus cuentas. Jorge fue víctima de un ataque cibernético en el que su número de celular fue duplicado y su información personal resultó vulnerada.



Consejo

Nunca compartas datos personales por mensajes o enlaces sospechosos ni introduzcas información sensible, como datos bancarios, si estás conectado a una red wifi pública.

Spear Phishing

Así empezó la estafa...

Luis recibió un mensaje a través de sus redes que parecía legítimo, sin pensarlo, compartió datos personales y de sus cuentas. Terminó siendo víctima de un fraude. **Ahora sabe que no debe compartir información personal ni sensible.**

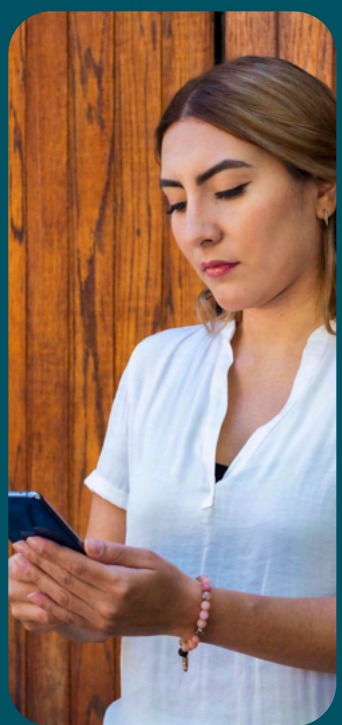
Consejo

Para evitar que vulneren tus cuentas, **activa el doble factor de autenticación** y evita dar clic en links que recibas por mensaje.

Vishing y Smishing

Así empezó la estafa...

Un supuesto ejecutivo del banco llamó a Ana para alertarla sobre cargos en su cuenta/tarjeta, además, le ofreció ayuda para bloquear su tarjeta y cancelar los cargos a través de un enlace que le compartieron por SMS. Al acceder le pidieron ingresar datos confidenciales y personales.
Ana compartió su información y fue víctima de fraude.



Consejo

Nunca compartas ningún tipo de información o códigos de seguridad (CVV) de tu tarjeta física o digital, códigos de NetKey®, etc. ni accedas a ligas que te lleguen por SMS.