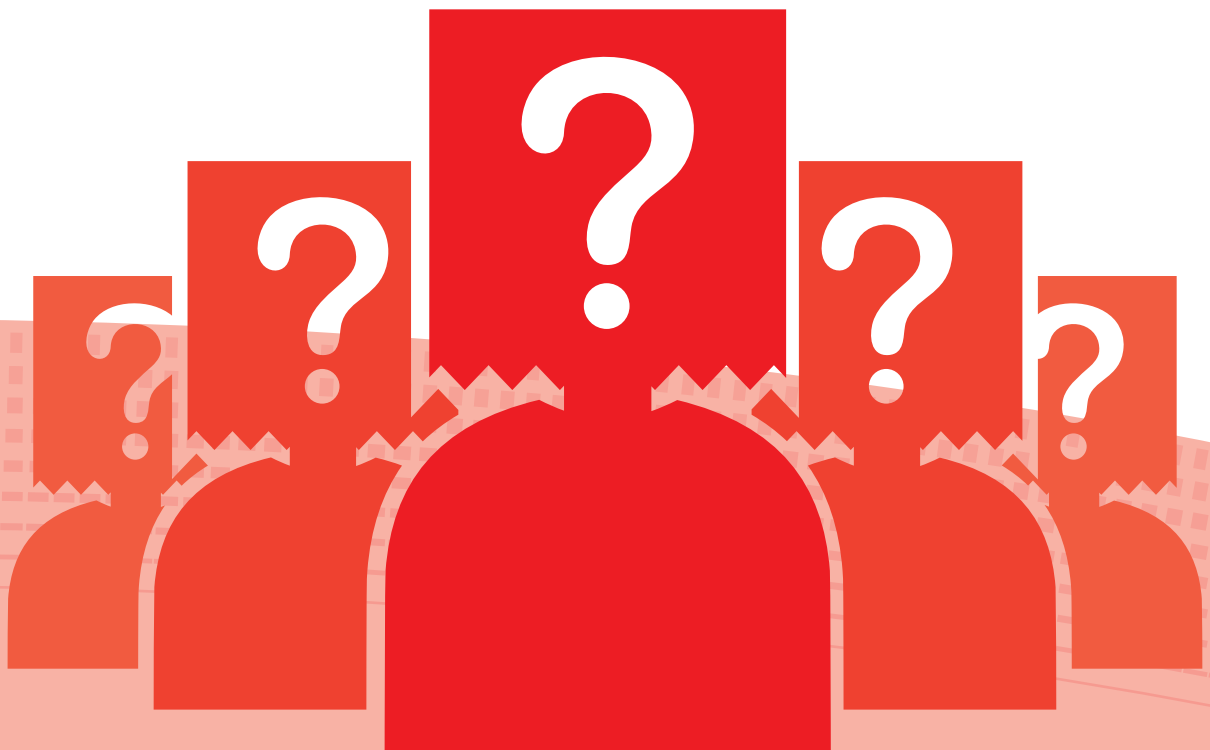
Llega a tu correo electrónico un mensaje de tu banco avisándote que tu cuenta de banca por internet ha sido bloqueada. ¿Qué haces?



a) Lo ignoro y doy aviso a mi banco.

b) Me preocupo y trato de comunicarme con mi banco.

c) Respondo de inmediato al correo llenando los datos que me solicitan.

Sin darte cuenta, todos los días realizas actividades financieras: consultar el saldo de tu plástico, comprar boletos para el cine por teléfono, pagar la cuenta en un restaurante con tarjeta de crédito, entre muchas otras, que al realizarlas revelan parte de tu información personal y financiera.

Los ladrones de identidad aprovechan esta información para cometer algún fraude en tu nombre, por eso es importante que estés alerta.

¿Qué es el robo de identidad?

Es cuando alguien roba tu información personal y financiera para suplantar tu identidad y obtener beneficios de forma fraudulenta. Cuando esto sucede, no sólo pierdes dinero, también se daña tu reputación financiera. Los ladrones emplean varios métodos para acceder a tu información, te decimos cómo evitarlos.

Phishing

Tratan de engañarte para que reveles información financiera mediante el envío de correos electrónicos que simulan ser de una institución legítima.

Para evitar que te pesquen: no respondas a ningún correo electrónico donde te soliciten información personal o financiera, ni hagas *clic* en los hipervínculos.

¡Ningún banco solicita información confidencial sobre tu cuenta a través de un correo electrónico! He aquí una muestra de este tipo de fraudes:

Clonación

Mediante un pequeño dispositivo (*skimmer*) los delincuentes copian y almacenan los datos de la banda magnética de tu tarjeta, esto cuando pagas o retiras dinero en un cajero automático.

La recomendación: nunca pierdas de vista tu tarjeta, por ejemplo, en restaurantes solicita que te lleven la terminal (TPV) a la mesa. En cajeros automáticos verifica que el lector de tarjetas no contenga dispositivos extraños.

Pharming

Te llega un correo electrónico, que al momento de abrirlo, instala un código en tu equipo personal, modificando determinados archivos, para que la próxima vez que ingreses al portal de tu banco te desvíen a sitios *web* falsos sin que te des cuenta.

¿Cómo prevenir este fraude? Instala en tu computadora paquetes de seguridad (*firewall, antispyware*) que te protejan contra virus y otras amenazas. Actualízalos con regularidad.

Vishing

Te llaman y una grabación te alerta de un supuesto fraude con tu tarjeta de crédito. Te indican un número telefónico al que debes llamar de inmediato. Cuando hablas, te responde otra grabación que te pide que ingreses, mediante el teclado telefónico, los datos de tu tarjeta.

¡Cuelga! si recibes una llamada donde te solicitan teclear tus datos o te piden información.

¿Y si ya caíste?

- Si detectas que tu identidad ha sido robada o que se ha hecho mal uso de tus datos financieros, denuncia el fraude ante el Ministerio Público.
- Si tu tarjeta de crédito fue clonada, cancélala de inmediato y acude al banco a resolver tu problema. Si no obtienes respuesta acude a Condusef.
- Si derivado de este fraude se reporta una mala nota en tu historial crediticio, presenta una solicitud de aclaración ante buró de crédito.

Otras medidas de seguridad

- Guarda los *vouchers* de las operaciones que realices con tu tarjeta de crédito o débito, para cualquier reclamación.
- Nunca apuntes tu NIP en tu tarjeta o lo guardes cerca de tu cartera.
- No dejes tus productos financieros (cheques, tarjetas) en tu auto, al usar un *valet parking* te los pueden clonar.
- Si una persona, un sitio *web* o un correo electrónico te prometen una oferta especial o un premio, utiliza el sentido común: si algo suena demasiado bueno para ser verdad, probablemente no lo es.