Hay mensajes que simulan provenir de tu banco preocupado por la seguridad de tu cuenta. Después de notificarte que tu servicio de banca electrónica ha sido suspendido, te piden que llenes un sencillo formulario para restablecerlo.

¡Cuidado!

Ningún banco solicita información confidencial sobre tu cuenta a través de un correo electrónico.

El *phishing*, un tipo de engaño creado por delincuentes, con el objetivo de obtener información como números de tarjetas de crédito, claves, datos de cuentas bancarias, etcétera. El objetivo es que caigas en la trampa para poder hacer compras o solicitar créditos a tu nombre.

¿Alguna vez te ha llegado a tu correo electrónico un mensaje de que ganaste un sorteo o de una princesa africana en desgracia, un alto funcionario de un banco europeo o el abogado de un millonario que ha fallecido sin dejar herederos?

El común denominador entre estos personajes tan contrastantes es que te prometen ganancias inmediatas.

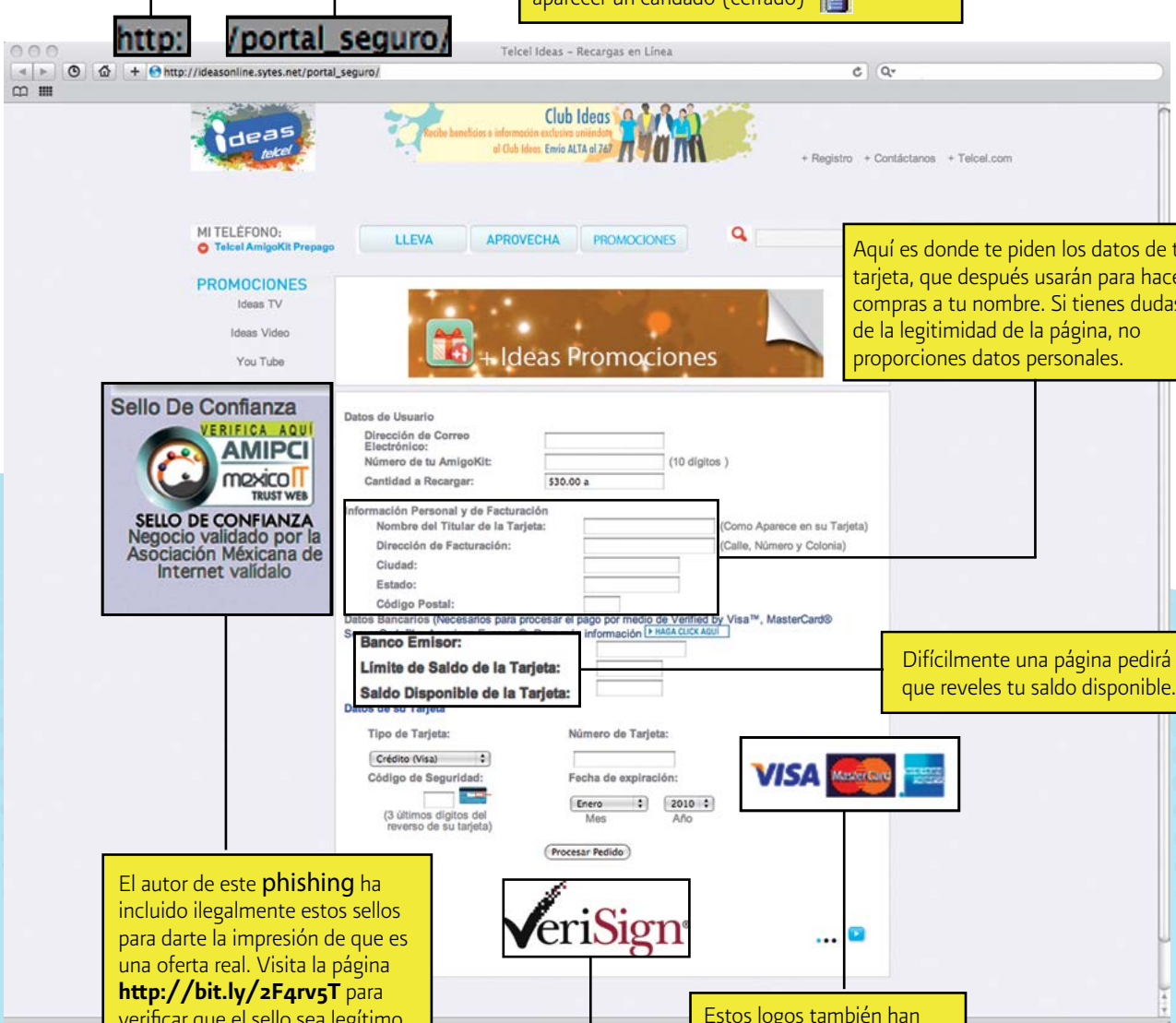
Detrás de estas acciones hay estafadores que te están lanzando un anzuelo para obtener los detalles de tu cuenta bancaria. Lo que ocurrirá es que tus datos serán utilizados para cometer un fraude.

¡Ten mucho cuidado! No reveles por correo electrónico información personal; mucho menos datos esenciales de tu cuenta (como el NIP o el código de seguridad de tu tarjeta).

¡Aprende a identificar correos fraudulentos!

En este ejemplo real recibes un correo de alguien que firma "Ideas Telcel", y que en el asunto propone: "Recarga saldo y recibe el doble!!!". Este correo te lleva a la página:

La terminación "portal seguro" no significa nada. Una página segura tendría que comenzar con "https". Y en la barra de estado debe aparecer un candado (cerrado)



Aquí es donde te piden los datos de tu tarjeta, que después usarán para hacer compras a tu nombre. Si tienes dudas de la legitimidad de la página, no proporciones datos personales.

Difícilmente una página pedirá que reveles tu saldo disponible.

El autor de este **phishing** ha incluido ilegalmente estos sellos para darte la impresión de que es una oferta real. Visita la página **http://bit.ly/2F4rv5T** para verificar que el sello sea legítimo.

Estos logos también han sido incluidos ilegalmente.

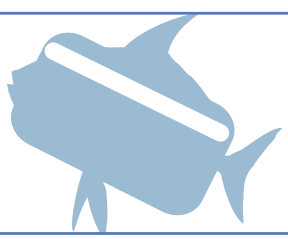
Evita los anzuelos

Usar una tarjeta de crédito para pagar productos y servicios por internet no entraña más riesgos que otras operaciones que puedas hacer con tu plástico, como cuando dispones de dinero en un cajero automático o cuando pagas en un restaurante.

Te damos 5 recomendaciones para no ser víctima de un fraude por internet y realizar tus compras con éxito:

1 Asegúrate de que se trata de un sitio legítimo

Investiga qué opinión tienen otros compradores en línea acerca del comercio donde quieres adquirir el servicio o producto que deseas. Existen incluso sitios de consumidores que tienen espacios destinados a recopilar opiniones acerca de empresas y proveedores. Prefiere aquellos comercios que cuentan con los sistemas de seguridad **Verified by Visa** y **MasterCard Securecode**.



2 Verifica que la dirección electrónica sea genuina

Revisa que la página donde realizarás el pago tenga en el protocolo una letra s (https o shttp) y que en la parte inferior o superior derecha de la barra de estado tenga el icono de un candado, lo que indica que se trata de un sitio seguro.

3 Busca sellos de aprobación de terceros

Hay sellos que pueden funcionar como indicador de que un sitio es legítimo y seguro, por ejemplo los de AMIPCI. Cuando veas estos sellos, cerciórate de que no estén falsificados: haz clic sobre la imagen para comprobar que están ligados a la organización que los avala.

4 Crea contraseñas fuertes

Las contraseñas son una llave de acceso a cuentas en línea, correos electrónicos, reservaciones; razón de más para que pongas mucho cuidado al crear contraseñas únicas y fuertes. Al respecto:

a) Procura no usar la misma contraseña para distintos servicios.
b) Evita usar contraseñas fáciles de adivinar como tu nombre, tu fecha de nacimiento, números telefónicos, series numéricas o alfabéticas (1234 o qwerty, por ejemplo).
c) No compartas las contraseñas con nadie.

5 Usa la tecnología a tu favor

Verifica que tu computadora cuente con:

a) Un antivirus. Los virus informáticos son programas maliciosos que pueden provocar daños en el **software** o en el **hardware** de tu computadora. Quizá tu equipo ya tenga un antivirus instalado, pero no te servirá del todo si no lo actualizas constantemente.
b) Un **firewall.** Es un programa que ayuda a proteger tu equipo y su contenido contra accesos no autorizados de extraños en internet.
c) Un **antispyware.** Evitará que puedan monitorear y registrar las actividades que realizas en internet o extraer información personal.

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO
CONDUSEF