NO TODO LO QUE BRILLA ES ORO

En la red hay cosas que no son lo que parecen. Cuando pase frente a ti una oportunidad de ganar dinero fácil, asegúrate de que no sea el camino más corto hacia una estafa.

DE LA **REDACCIÓN**

Los caminos de la red son misteriosos. Si revisas tu cuenta de correo electrónico, es probable que encuentres un mensaje firmado por 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 necesitan mover grandes cantidades de dinero y para hacerlo requieren tu ayuda. En el mensaje te explican su situación en dos o tres líneas, y te prometen una jugosa recompensa si aceptas auxiliarlos.

Otra variante es un mensaje que te notifica que acabas de ganar millones en la lotería, o que te has hecho acreedor a un premio por ser la persona número cinco millones en ingresar a una página electrónica. Y finalmente hay otros mensajes (de los que te presentamos un ejemplo real en la página 26) que simulan provenir de funcionarios de tu banco preocupados 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.

Detrás de estas acciones no hay princesas, ni banqueros, ni millonarios: hay estafadores que te están lanzando un anzuelo para obtener los detalles de tu cuenta bancaria. En ocasiones te piden que pagues por adelantado una tarifa o un impuesto para completar el hecho, y te dan detalles que parecen reales. Lo que ocurrirá es que perderás ese dinero y tus datos bancarios serán utilizados para cometer otros fraudes.

En internet abundan los sitios que no son lo que parecen. Auténticas trampas que hacen de la clonación de tarjetas y el robo de identidad amenazas constantes. Pero lo cierto es que 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. Para hacer pagos más seguros en línea, sigue estas recomendaciones:

Asegúrate de que se trata de un sitio legítimo: investiga qué opinión tienen otros compradores en línea acerca del servicio o pro-

ducto que deseas pagar. Existen incluso sitios de consumidores que tienen espacios destinados a recopilar opiniones acerca de empresas y proveedores.

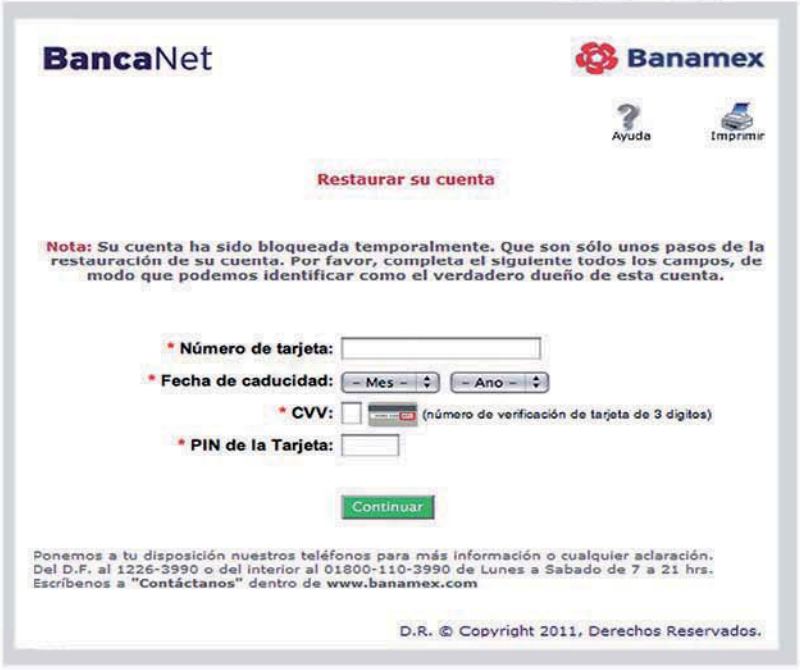
Verifica que la dirección electrónica sea genuina: revisa que la página donde realizarás el pago tenga en el protocolo una letra "s" (https o shttp) y que en la parte inferior derecha, en la barra de estado, tenga el ícono de un candado, o una llave entera, lo que indica que la información de la operación de compra está encriptada o protegida, y por lo tanto se trata de un sitio seguro.

Busca sellos de aprobación de terceros: hay algunos sellos que pueden funcionar como indicador de que un sitio es legítimo y seguro, por ejemplo los de AMIPCI, *Verified by Visa* y *Mastercard*. 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.

El Sello de Confianza AMIPCI es un distintivo otorgado por la Asociación Mexicana de Internet para sitios en México. Cuando haces clic en el sello electrónico, debe desplegarse un certificado digital adjunto que reconoce a los negocios o instituciones que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidos. **Es muy importante que verifiques que la dirección a la que fue otorgado el certificado coincida con el sitio que la ostenta.**

Defiende tu privacidad: muchos sitios de ventas en línea requieren que te inscribas creando un nombre de usuario y una contraseña (*Log-in*). Buena parte de ellos solicitan datos reales y personales en sus formularios de registro, además de pedirte información sobre tus hábitos de recreación o de consumo. Cuando te encuentres en esta situación, aporta sólo los datos estrictamente necesarios. Los campos obligatorios generalmente aparecen marcados con un asterisco (*). Nunca respondas preguntas que no consideres apropiadas para la transacción.

¡Cuidado! Ningún banco solicita información confidencial sobre tu cuenta a través de un correo electrónico. Este es un ejemplo real de un correo fraudulento:


BancaNet

Banamex

Ayuda Imprimir

Restaurar su cuenta

Nota: Su cuenta ha sido bloqueada temporalmente. Que son sólo unos pasos de la restauración de su cuenta. Por favor, completa el siguiente todos los campos, de modo que podemos identificar como el verdadero dueño de esta cuenta.

* Número de tarjeta:

* Fecha de caducidad: - Mes - - Ano -

* CVV: (número de verificación de tarjeta de 3 dígitos)

* PIN de la Tarjeta:

Continuar

Ponemos a tu disposición nuestros teléfonos para más información o cualquier aclaración. Del D.F. al 1226-3990 o del interior al 01800-110-3990 de Lunes a Sabado de 7 a 21 hrs. Escríbenos a "Contáctanos" dentro de www.banamex.com

D.R. © Copyright 2011, Derechos Reservados.

Crea contraseñas fuertes: las contraseñas son una llave de acceso a cuentas en línea, correos electrónicos, reservaciones y otra información importante, razón de más para que pongas mucho cuidado al crear contraseñas únicas y fuertes. Al respecto te sugerimos que:

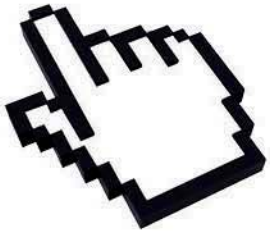
a) Procures no usar la misma contraseña para distintos servicios.

b) Evites usar contraseñas fáciles de adivinar como tu nombre, tu fecha de nacimiento, números telefónicos, series numéricas o alfabéticas (1234 o qwerty, por ejemplo), así como nombres de mascotas.

c) No compartas las contraseñas con nadie.

Usa la tecnología a tu favor:
a) 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* personal es un programa que ayuda a proteger tu equipo y su contenido contra accesos no autorizados de extraños en internet. Cuando se configura apropiadamente, detiene todo el tráfico no autorizado hacia y desde tu computadora.



Medidas de seguridad personales

- Activar alertas de movimientos de cuenta, ya sea por correo electrónico o por SMS (teléfono celular).
- Utilizar un *firewall*: **www.zonelabs.com, www.symantec.com.mx, www.mcafee.com.mx**, entre otros.
- No utilizar computadoras en lugares públicos para realizar operaciones financieras.
- Utilizar un programa *antispyware*, esto evitará que puedan monitorear y registrar las actividades que realizas en internet o extraer información personal: *McAfee, AdAware, Spyware Doctor* y *Microsoft Windows Defender*, entre otros.
- No compartir claves de acceso (contraseñas, NIP, etcétera).
- Actualizar el antivirus de la computadora.
- No utilizar nombre, fecha de nacimiento y números telefónicos, como contraseña.
- No utilizar la misma contraseña para distintos servicios y cambiarlas periódicamente..
- Verificar día a día los movimientos y saldos de la cuenta.