

PROTEJA SU INFORMACIÓN Y DOCUMENTOS PERSONALES

El fraude electrónico (phishing) es una estafa moderna para aprovechar las nuevas tecnologías.

El fraude electrónico utiliza promociones por correo electrónico, teléfono o Internet en el cual los ladrones simulan representar empresas legítimas. Utilizan información perturbadora o emocionante para exigir una respuesta urgente en un intento por engañar al usuario para que revele información personal. Este tipo de correos electrónicos falsos solicitarán los números de cuenta o de PIN.

Los estafadores cibernéticos (Pharmers), redirigen a usuarios desprevenidos de Internet desde un sitio web comercial hacia un sitio malicioso que imita al sitio legítimo.

Esto se logra mediante un "enlace incorporado" que simula ser un sitio seguro. Cuando los usuarios ingresan su nombre y contraseña, los delincuentes pueden capturar la información.

Consejos para el Uso de la Computadora

- Nunca utilice una computadora de uso público para sus transacciones financieras
- Instale software de protección antivirus y actualícelo con frecuencia
- Tenga cuidado con los correos electrónicos que abra
- Busque sitios web que comiencen con https://
- Busque un ícono de un candado o una llave entera



Servicios Policiales de Riverside
Para informar sobre un delito:

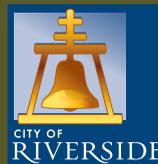
**SOLO EMERGENCIAS
LLAME AL 911**

**NO EMERGENCIAS
787-7911**

mayor información en línea en:
rpdonline.org



SERGIO G. DIAZ
JEFE DE LA POLICÍA



City of Arts & Innovation

El Departamento de Policía de Riverside y los habitantes de la Ciudad trabajando juntos para evitar el delito



**Robo de
Identidad**



Integridad Servicio Excelencia

¿QUÉ ES EL ROBO DE IDENTIDAD?

El robo de identidad se produce cuando alguien se apodera de información personal como un número de tarjeta de crédito, de licencia de conducir, de certificado de nacimiento o de seguro social o información bancaria sin autorización.

¿COMO OBTIENEN ELLOS SU IDENTIDAD?

Espiando sobre el Hombro en Cajeros Automáticos (ATM en inglés)

Los ladrones observan los Números de Identificación Personal (PIN), números de tarjetas de crédito o contraseñas.

Hurgando o extrayendo la basura de los contenedores de reciclaje y bolsas de basura transparentes:

Los ladrones echan un vistazo a la basura buscando solicitudes de créditos, estados de cuenta de tarjetas de crédito, documentación financiera y otra información personal.

Robo de propiedad personal

Los objetos como billeteras, monederos y vehículos contienen información privada. Las computadoras contienen información sobre los sitios web visitados, correos electrónicos personales y posiblemente información financiera.

Skimming o Adulteración

Se produce en cajeros automáticos y terminales de puntos de venta. Los ladrones pueden leer los números de tarjeta de crédito o débito y número de identificación personal (PIN) mediante un dispositivo de almacenamiento de información llamado skimmer (dispositivo que permite capturar la información de la banda magnética de la tarjeta junto con una cámara que captura la clave ingresada). Los ladrones a menudo pueden recabar información que puede ser usada para reproducir tarjetas para su uso personal en detrimento suyo.

Compra de Información

Los números de cuentas son robados por empleados deshonestos que trabajan para instituciones financieras o empresas que procesan información financiera, trabajadores de negocios de venta al público o consultorios médicos. Los registros robados se pasan o venden en salas de chat o sesiones de mensajería instantánea. Algunas veces se viola la seguridad de las empresas, poniendo en riesgo su información personal.

Casillas de Correo

Los ladrones retiran el correo de las casillas de correo o hacen que se reenvíe a otro domicilio. Están buscando nuevas tarjetas de créditos, ofertas de créditos pre-aprobados, resúmenes bancarios, información impositiva o documentos de inversiones y ganancias.



Fuentes Públicas

Fuentes como periódicos (obituarios), guías telefónicas y registros gubernamentales de acceso público son revisadas para obtener información con fines fraudulentos.

Proteja su información y documentos personales

- En caso de pérdida o robo de un certificado de nacimiento, licencia de conducir, pasaporte, tarjeta bancaria (de débito) o de crédito, notifique INMEDIATAMENTE al emisor y a la policía
- Reduzca o destruya los documentos personales confidenciales antes de reciclarlos
- Cúbrase al ingresar su PIN y nunca se lo diga a otra persona. No use su dirección, teléfono o número de seguro social (SIN, Social Insurance Number) como PIN
- Asegure su casilla de correo de ser posible con llave, o use una casilla postal. Registre la fecha en que debe recibir sus facturas, estados financieros o tarjetas de crédito. Notifique a la empresa si no llegan en los plazos previstos. Cuando se ausente de la ciudad, haga que una persona de confianza recoja su correo o utilice el servicio de retención de correo en la oficina de correos
- Controle los resúmenes y registros financieros para detectar irregularidades
- Guarde fotocopias de sus tarjetas de crédito. Esto le ayudará a avisar a la empresa en caso de que pérdida o robo
- No lleve con usted documentos como certificados de nacimiento, pasaportes o tarjetas de Seguro Social, salvo que sea necesario
- Proteja su computadora con una contraseña de encendido que solo usted conozca. No use las funciones de ingreso automático que guardan su nombre de usuario y contraseña

El Robo de Identidad es un delito de consumo de rápido crecimiento en Norteamérica



GO TO PRINT

**Marketing Group
EXTERNAL ROUTING**

DATE: 4/12/11

REQ. DEPT.: RPD CSB

DEPT. CONTACT: Officer Jeff Maier

APPROVED **NOT APPROVED**

APPROVED WITH CHANGES

DEPT. DIRECTOR: _____