VOLUME 9, ISSUE 2

"COMMITTED TO DEBT FREE GUIDANCE"

GOLDEN STATE DEBT MGMT
MARCH 2014 NEWSLETTER

How Fraudsters Might Use Stolen Personal Information

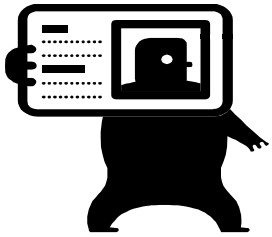
Due to recent cyber attacks on at least 2 large retail chains, over 100 million consumers have had their personal data exposed to potential fraud.

CONSUMER PERSONAL DATA IS SOLD ON THE INTERNET TO THIEVES WHO USE THE INFORMATION IN THE FOLLOWING WAYS:

Apply for credit cards accounts using your stolen personal information (this could lead to time-consuming activities and significant costs to resolve ID theft-related negative credit reporting).

Make unauthorized purchases on consumer credit card accounts (although you are protected from liability on credit card fraud, you still have to locate and report the unauthorized purchases).

Use email addresses for phishing scams (looking for victims to rip-off). Usually phishing emails are routed to spam folders; however, when curious consumers open unfamiliar emails and follow unknown links or download free programs, they can become victims of malicious software programs, such as spyware, trojans, worms, etc.



Ways to Protect Yourself Form Professional Identity Thieves

Install security software on your computers and keep it up-to-date. (you can do a Google search on "the best computer security software programs" to find expert reviews, which list and rate computer security software products).

Make sure you have the most recent web browser version on your computer (example. Internet Explorer, version 11, for Windows 7).

Be suspicious of, and avoid opening, any emails you receive advising you to act immediately by clicking an unknown link. (fake email messages are formulated to seem like they were sent by a legitimate organization, using a familiar email subject headline, such as the name of your banking institution or credit card issuer).

MORE ABOUT ID FRAUD

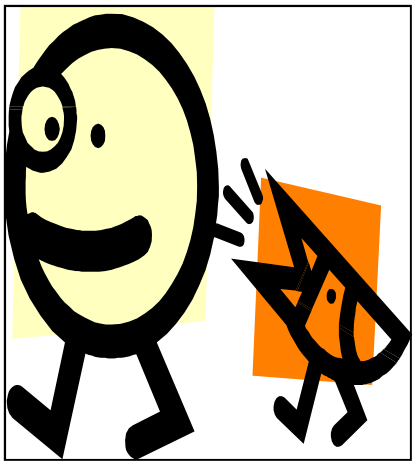
The widespread convenience of using the Internet to conduct consumer activities like buying a product or service, using phones, tablets and computers, has exposed us to become easier targets as victims to id fraud.

Stolen consumer information can be used to gain access to household services, such as electricity and natural gas; landlines and cell phones; and Internet, cable and satellite access.

Stolen personal data can be used for almost any type of id fraud, including applying for social services such as welfare benefits, disability, social security income, and other government-related distress assistance.

Finally, bank fraud is probably the most dangerous type of id theft, due to bank accounts linked to debit cards, are subject to unlimited loss, in certain instances, such as if the fraud is not reported to your banking institution within 2 months.

Better Password Protection



Preventing thieves from easy access to you bank accounts and computers.

For convenience some consumers use simple passwords such as "admin", "123456" or "password."

For better security, create longer passwords, using numbers & letters. Save them on a memory stick.

Another option is to use a password manager program, which creates and saves passwords for you. Also, it encrypts your password database. Then, all you will need to memorize is the master password.

Limiting Your Expenditures

Avoid late fees, save on stamps and track creditor payments by paying your bills online.

Every pay period, transfer funds from your paycheck to a non-linked savings accounts.

Consider waiting at least 2 weeks before committing to a major purchase to limit impulse buys.

Develop the habit of tracking your expenses; begin by monitoring & writing down all purchases you make during a 1 week period.

VOLUMEN 9, EDICION 2

"DEDICADOS A LIQUIDACION DE DEUDA"

GOLDEN STATE DEBT MGMT

BOLETÍN DE NOTICIAS DE MARZO 2014

Cómo Defraudadores Utilizan Información Personal Robada

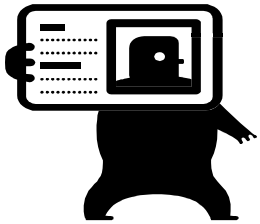
Debido a recientes ataques cibernéticos, más 100 millones de consumidores han tenido sus datos personales expuestos a posibles fraudes.

DATOS PERSONALES DE CONSUMIDOR SE VENDEN EN EL INTERNET A CRIMINALES QUE USAN LA INFORMACION PARA LO SIGUIENTE:

Solicitan abrir cuentas de tarjetas de crédito usando su información personal (esto podría causarle desperdicio de tiempo y costos significativos para resolver crédito dañado debido al robo de identidad).

Hacer compras no autorizadas de tarjeta de crédito (aunque usted está protegido sobre responsabilidad en el fraude de tarjeta de crédito, necesita localizar e reportar las compras no autorizadas).

Usar correo electrónico para iniciar fraudes de phishing (busca de víctimas para estafa). Cuando consumidores abran correo electrónico y siguen enlaces desconocidos o descargaran programas extraños, pueden ser víctimas de programas de software maliciosos como spyware, que atacan su computadora y roban su datos.



Previniendo Robo de Identidad

Instale un programa de seguridad en sus computadoras y mantenerlo actualizado. (haga búsqueda de Google de "mejores programas de seguridad informáticos" para localizar comentarios expertos, que evalúan productos de seguridad informática.

Verifique que tiene la versión más reciente del navegador web en su computadora (ej. Internet Explorer 11, para Windows 7).

Sospeche y evite abrir correo electrónicos que recibe pidiéndole actuar de inmediato haciendo clic en un enlace desconocido (mensajes de correo electrónico falsos parecen que están enviados por organizaciones legítimas, usando titulares familiares, como el nombre de su institución bancaria o uno de sus acreedores).

MAS SOBRE EL ROBO DE IDENTIDAD

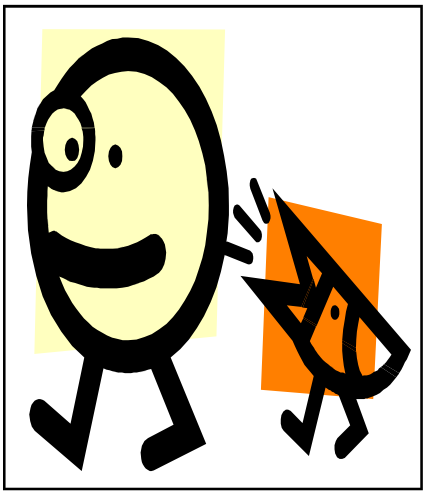
La comodidad del uso de Internet para conducir actividades de consumidor, como la compra de un producto o servicio, usando teléfonos, tabletas y computadoras, nos ha expuesto a ser fácil víctimas al robo de identidad.

Datos personales robados pueden ser usados para tener acceso a servicios domésticos, como para electricidad y gas natural; teléfono de hogar y celulares; y acceso a Internet, cable y satélite.

Datos personales robados pueden ser usados para cualquier tipo de robo de identidad, como para solicitar beneficios de seguridad social, discapacidad y otras asistencias dado por el gobierno.

El fraude bancario es el tipo de robo de identidad más peligroso, debido a que las cuentas bancarias ligadas a tarjetas de débito pueden ser sujeto a pérdida ilimitada, si usted no reporta el fraude a su banco dentro de 2 meses.

Mejor Protección de Contraseña



Prevenga El Fácil Acceso A Cuentas Bancarias y Computadoras.

Para comodidad algunos de nosotros usamos contraseñas simples como "1111", "123456" y "abc123."

Para mejor seguridad, crea contraseñas más largas, usando números y letras e guardarlos en memoria USB.

También puede utilizar un programa contraseña administrador (**Password Manager**) que crea y guarda contraseñas para usted. Además, encripta su base de datos de contraseñas. Luego, solo necesita memorizar una contraseña principal.

Limitando Sus Gastos

Evite cargos por pagos atrasados, ahorre en sellos y monitoree pagos de acreedor haciendo pagos por Internet.

Cada período de pago, transferir fondos de su salario a una cuenta de ahorros no ligada.

Considere esperar 2 semanas antes de hacer compras costosas para limitar la compra de impulso.

Desarrollar el hábito de monitorear sus gastos anotando todas compras hechas durante un 1 semana.