

Money Matters: Minimizing your identity theft risks

NOTES TO EDUCATORS: This release is part of the Money Matters series offered by the Family Financial Education Team. Six of the releases are now offered in Spanish, along with a cover letter for newspaper editors. This release will not be sent to statewide media. Please add local contact information and remember to alter the quotes if you substitute your own name in the release. An optional sidebar focuses on home computer protection. You are welcome to submit these articles to local Spanish language newspapers, newsletters or other Spanish language communications as appropriate. For more information, contact Faden Fulleylove-Krause at 920-849-1450 or faden.fulleylove-krause@ces.uwex.edu.

Para ser publicado: junio 2005

Persona de contacto: Brenda Janke, 715-536-0304, brenda.janke@ces.uwex.edu

Los Asuntos de Dinero:
Cómo disminuir los riesgos del robo de identidad

[YOUR TOWN / EI PUEBLO O CIUDAD DONDE USTED VIVE] MADISON, Wis.—En lo que se refiere al robo de identidad, usted no puede controlar todas las circunstancias, pero hay cosas que usted puede hacer para disminuir el riesgo.

Empiece por pedir una copia de su informe crediticio. Una enmienda a la Fair Credit Reporting Act (Ley de Notificación Justa de Crédito) requiere que las tres compañías mayores de informes del consumidor le den a usted una copia gratis de sus informes crediticios, cuando usted las pida, cada 12 meses.

Para pedir su informe anual gratis de una o de todas las compañías de informes del consumidor, visite www.annualcreditreport.com, llame gratis al 877-322-8228 o imprima un Annual Credit Report Request Form (Formulario para el Pedido del Informe Crediticio Anual) en ftc.gov/credit. No se comunique individualmente con ninguna de las tres compañías. Si usa la web, asegúrese de que está en el sitio oficial; evite los sitios fraudulentos que tienen direcciones electrónicas similares. Usted puede pedir que solamente los últimos cuatro dígitos de su número de seguro social aparezcan en sus informes crediticios.

La U.S. Federal Trade Commission (Comisión Federal de Comercio de los Estados Unidos) le recomienda que se proteja contra el robo de identidad.

Use contraseñas con sus tarjetas de crédito, con su banco y con sus cuentas telefónicas. Evite usar información que se pueda obtener fácilmente, como el nombre de soltera de su madre, su fecha de nacimiento, los cuatro últimos dígitos de su número de seguro social o su número de teléfono. Si el uso de la cuenta requiere el nombre de soltera de su madre, pida que le permitan usar una contraseña en su lugar.

Pida información sobre los procedimientos de seguridad donde usted trabaja o en los establecimientos comerciales, las oficinas médicas u otras instituciones que requieren su información personal. Averigüe quién tiene acceso a la información y verifique que se maneje en forma segura. Si su información será compartida, pregunte cómo se mantendrá

la confidencialidad. Comenzando el primero de junio, una nueva ley federal requiere que los negocios y los individuos tomen medidas apropiadas para disponer de la información personal que contienen los informes crediticios.

No dé su información personal por teléfono, por correo o en el Internet a menos que usted inicie el contacto o conozca a la persona con la cual se está comunicando. Los ladrones de identidad se han hecho pasar por representantes de bancos, proveedores de servicios en el Internet e incluso agencias gubernamentales para conseguir que la gente revele su información de identidad. Antes de compartir información personal, confirme que usted está comunicándose con una organización legítima. Consulte el sitio web de una organización escribiendo la dirección electrónica en vez de cortarla y pegarla. Llame al servicio para clientes al número que aparece en su estado de cuenta para verificar si necesitan su información personal. No use su teléfono celular para dar información, como por ejemplo, su número de seguro social.

Tenga cuidado con su correo y con su basura. No tire simplemente todo el correo no solicitado; muchas de estas cartas incluyen información privada. Corte o triture recibos de cargos de tarjetas de crédito, solicitudes de crédito, formularios para el seguro, cuentas del médico, cheques y estados de cuenta del banco, tarjetas de crédito que han expirado y ofertas de crédito. Si no quiere recibir ofertas de crédito por correo, llame al 1-888-5-OPTOUT (1-888-567-8688). (Se le pedirá su número de seguro social porque las compañías de informes del consumidor lo necesitan para identificar su archivo.) Tenga cuidado al responder a promociones. Es posible que los ladrones de identidad creen ofertas falsas para obtener su información personal.

Deposite el correo que va a enviar en buzones postales o en la oficina de correos en vez de ponerlo en un buzón que no es seguro. Saque el correo de su buzón lo más pronto posible. Si piensa viajar y no podrá recoger su correo, llame al U.S. Postal Service (Servicio Postal de los Estados Unidos) al 1-800-275-8777 para pedir que le retengan su correo durante su ausencia. La oficina de correos local guardará el correo hasta que usted pueda recogerlo o hasta que vuelva a su casa. Recoja sus cheques nuevos en el banco en vez de que se los manden por correo.

No lleve consigo la tarjeta de seguro social; déjela en un lugar seguro. Lleve solamente la identificación y las tarjetas de crédito o las tarjetas débito que va a necesitar cuando salga. Haga copias de las tarjetas que usted lleva en su billetera para tener la documentación en caso de robo o pérdida. Cuando firme un recibo de una tarjeta de crédito, siempre verifique que el nombre impreso en el recibo es el suyo. Asegúrese de que nadie tome una fotografía de su cheque o tarjeta de crédito con la cámara fotográfica de un teléfono celular.

Dé su número de seguro social solamente cuando sea absolutamente necesario y pregunte si puede usar otros tipos de identificación. No use su número de seguro social como el número para su licencia de manejar o como el número de la póliza del seguro de salud. Su empleador y las instituciones financieras necesitarán su número de seguro social para informar sobre sus sueldos e impuestos. Otros negocios pueden pedirlo para obtener un informe crediticio cuando usted solicita un préstamo, desea arrendar un apartamento o se registra para los servicios públicos. Sin embargo, es posible que solamente necesiten el número para la documentación general.

Por último, pero no por ello menos importante, no deje que el miedo al robo de identidad controle su vida. Aunque las precauciones presentadas anteriormente parecen ser muchas, estos consejos intentan solamente animarnos a que estemos vigilantes y ayudarnos a usar tácticas de seguridad basadas en el sentido común para resguardar nuestra información personal.

Un folleto gratis llamado “Identity Theft: Your Good Name Gone Bad!” (El robo de la identidad: ¡Su buen nombre arruinado!) y otras publicaciones están disponibles en español e inglés en Call for Action (Llame para la acción) al 1-800-647-1756 o en línea en www.callforaction.org. Para saber más sobre el manejo de las finanzas familiares, comuníquese con la oficina de la UW-Extensión en su condado [ADD LOCAL CONTACT INFORMATION / AÑADA LA INFORMACIÓN DE CONTACTO LOCAL].

###

<http://www.uwex.edu/ces/news>

Archivo: Consumer Issues, Family financial management, Finance (Problemas del Consumidor, Manejo de las Finanzas Familiares, Finanzas)

SIDEBAR:

La computadora en su casa y las preocupaciones del robo de identidad

Según el uso que usted haga de su computadora, es posible que un ladrón de identidad no necesite entrar en su casa para robar su información personal. Janke [YOUR NAME/ SU NOMBRE] ofrece las siguientes recomendaciones de la Federal Trade Commission (Comisión Federal de Comercio) para proteger su identidad en línea.

-- Actualice su programa de protección contra virus con regularidad e instale parches para su sistema de operación y para otros programas para proteger contra intromisiones e infecciones que pueden poner en peligro los archivos o contraseñas de su computadora. Idealmente, el programa de protección contra virus debe ser ajustado para que se actualice automáticamente una vez a la semana. El sistema de operación Windows XP también puede ser ajustado para que busque parches y los baje automáticamente.

No abra archivos que han sido enviados por correo electrónico por personas que usted no conoce, ni haga clic en hipervínculos (hyperlinks) ni baje programas de gente que no conoce. Tenga cuidado al usar programas que comparten archivos. El abrir un archivo podría exponer su sistema a un virus de computadora o a un programa que se conoce como “spyware” que podría capturar sus contraseñas o cualquier otra información que usted escriba con el teclado de su computadora.

-- Use un programa de cortafuegos (firewall), especialmente si usa una conexión al Internet de alta velocidad como cable o DSL que conecta su computadora al Internet 24 horas al día. El programa cortafuegos le permite detener el acceso no autorizado a su computadora. Sin él, los piratas informáticos (hackers) pueden apoderarse de su computadora, obtener acceso a la información personal que se guarda ahí o usarla para cometer otros crímenes.

-- Use un buscador (browser) (programa que codifica la información que usted manda a través del Internet) seguro para proteger sus transacciones en línea. Cuando entregue información, busque el icono del candado en la barra de estado del buscador para asegurarse de que su información esté segura durante la transmisión.

-- No guarde información financiera en su computadora portátil a menos que sea absolutamente necesario. Si lo hace, use una contraseña hermética con una combinación de letras (mayúsculas y minúsculas), números y símbolos. Una buena manera de crear una contraseña es pensar en una frase fácil de recordar y usar la primera letra de cada palabra para su contraseña, cambiando algunas letras a números que parecen letras. Por ejemplo, "I love Felix; he's a good cat," se convertiría en 1LFHA6c ("Amo a Felix; es un buen gato = AaFEUB6). No use el registro (log-in) automático que guarda su nombre de usuario y su contraseña y siempre termine la sesión. De esta manera, si le roban su computadora portátil, es más difícil para un ladrón obtener acceso a su información personal.

-- Antes de disponer de una computadora, borre toda la información personal que contenga. Es posible que no sea suficiente borrar los archivos usando los mandatos del teclado o del ratón o reformatear el disco duro porque los archivos pueden quedarse en el disco duro de la computadora y pueden ser retirados fácilmente. Use un programa de utilidad para limpiar el disco duro completamente.

-- Tenga cuidado al usar una conexión inalámbrica para transmitir información personal o bancaria. Las conexiones inalámbricas pueden ser interceptadas si no han sido instaladas correctamente.