Oficina del
Fiscal General

Seguridad en Internet

(Internet Safety)

AGOSTO DEL 2005

LAWRENCE WASDEN
FISCAL GENERAL
Edificio Capitolio del Estado
Boise, Idaho 83720-0010
www.ag.idaho.gov

Estado de Idaho
Oficina del Fiscal General
Lawrence Wasden

Estimado habitante de Idaho:

La Internet es una herramienta apasionante que le presenta enormes cantidades de información al alcance de su mano. Con un toque del ratón (*mouse*), puede comprar pasajes aéreos, utilizar herramientas de búsqueda, conversar con los amigos o participar en juegos interactivos.

Pero también existen riesgos en la Internet, por lo tanto, es importante ser ciber-inteligente y que su experiencia en línea sea segura. Es de suma importancia que los padres supervisen el uso de la Internet por parte de sus hijos. Como lo hemos advertido con frecuencia, los niños confiados son particularmente vulnerables a los predadores sexuales y a otros ciber-criminales.

Cuando usted entre en línea, tenga en cuenta su seguridad financiera y personal, su protección y privacidad. Además, debe acercarse con precaución a las “oportunidades de negocios” en línea y ser cauteloso

con las estafas de Internet y los virus de las computadoras.

Mi despacho ha preparado esta publicación para ayudarle a disfrutar de manera segura la Internet. Espero que le sea útil.

LAWRENCE G. WASDEN
Fiscal General

Tabla de contenido

SEGURIDAD Y PROTECCIÓN

La Internet ha abierto un nuevo mundo para muchas personas. A su disposición encontrará información, comunicación, incluso oportunidades de realizar compras al por menor en puntos de fábrica distantes. No obstante, existen graves riesgos asociados con el correo electrónico, navegar y hacer negocios en línea.

Uno de los más grandes riesgos es el hecho de que la Internet es un lugar anónimo donde no hay contacto cara a cara. Ladrones y depredadores se aprovechan de este anonimato y fingen ser alguien diferente de quien realmente son.

Estos consejos pueden garantizarle la seguridad en Internet.

COMPRAS EN LÍNEA

Utilice un navegador seguro

Un navegador es el software o programa que usted utiliza para explorar la Internet. Su navegador debe cumplir con los estándares de seguridad industriales, tales como, la Transacción Electrónica Segura (sigla en Inglés *SET*) Estos estándares cifran o modifican la información de compra que usted envía a través de la Internet, garantizando la seguridad de su transacción. La mayoría de computadoras vienen con un navegador seguro ya instalado.

Usted puede determinar si su navegador es seguro desde la ventana de su navegador. Seleccione la opción "AYUDA" del menú y luego seleccione "ACERCA DE". La información aparece y le muestra el nivel de codificación.

Si usted no tiene un navegador seguro, hay muchos de donde elegir. Los navegadores más comunes incluyen *Netscape Navigator* y *Microsoft Internet Explorer*. Usted puede descargar estos navegadores gratis desde Internet.

Cuando compra en línea, también es importante que compre desde un sitio seguro. Para mayor información ver "seguridad de los sitios de Internet" en la pagina 11.

Compre con compañías que usted conoce.

Cualquier persona puede montar un negocio casi con cualquier nombre en Internet. Si no conoce un negocio, busque la dirección física, el número telefónico y la dirección de correo electrónico. Póngase en contacto con el negocio y pida un folleto o un catalogo de mercancías y servicios. Pida una copia de la política de devoluciones y reembolsos del negocio. Comuníquese con la oficina de *Better Business Bureau* y la Agencia de Protección al consumidor en el estado de la oficina cede del negocio para averiguar que clase de antecedentes tiene el negocio. Si realiza una compra de un objeto desde una subasta a través de Internet, revise la evaluación de reacción del vendedor.

Antes de realizar una compra, asegúrese de que sabe por lo que está pagando. Revise la descripción, información de precios y cualquier limitación sobre las compras (por ejemplo bienes que puede ser que no estén disponibles para ser enviados fuera del país; puede que haya cantidades mínimas para hacer un pedido; etc.)

Revise la letra pequeña y busque palabras como “restaurado”, “liquidación”, “descontinuado” o “sin marca”.

Revise si el precio que aparece está en dólares estadounidenses o en otra moneda. Examine los requisitos de impuestos, o derechos sobre las compras, así como los costos de envío y de manejo y transporte.

Revise la política de privacidad de la compañía. La política debe decir que información se recolecta, cómo se va a usar y si la información se compartirá con otras personas.

Si tiene preguntas acerca del objeto a comprar o cualquiera de los costos o políticas, envíe un correo electrónico o llame por teléfono al vendedor.

Guarde una copia impresa de su compra

Cuando ordene algo a través de la Internet, guarde una copia impresa de su orden de compra, recibo o número de confirmación. Un registro escrito la ayudará a resolver cualquier problema relacionado con su compra.

Si paga con tarjeta débito o crédito, su transacción está protegida bajo la ley de facturación de crédito justa. Esta ley le otorga al consumidor el derecho de presentar cargos bajo ciertas circunstancias y de retener temporalmente el pago sobre los cargos disputados mientras se realiza una investigación. Si usted paga con tarjeta de crédito o débito, existen protecciones por pagos no autorizados bajo la *federal Electronic Fund Transfer Act*. Para mayor información sobre estas leyes, comuníquese con la Unidad de protección al consumidor del Fiscal General.

Si usted compra un objeto a través de una subasta por Internet y el vendedor no acepta tarjetas de crédito, considere usar un servicio de entrega en depósito. Si el vendedor sólo acepta cheques de gerencia o giros postales, decida si desea tomar el riesgo de enviar su dinero antes de recibir el producto. Asegúrese de seguir los pasos para proteger su privacidad – no de su información personal y confidencial como su número de seguro social, número de licencia de manejar o número de cuenta bancaria.

La ley acerca de los pedidos de mercancía por teléfono o por correo también cubre las compras realizadas a través de la Internet. A menos que se indique de otra manera, esta ley requiere que la mercancía sea enviada dentro de un plazo de 30 días. La compañía debe notificarle si la mercancía no se le puede enviar dentro de ese tiempo límite.

CONTRASEÑAS

Muchos sitios de Internet le solicitan que se registre y cree una contraseña para futuros accesos. Al crear una contraseña, el Consejo nacional de prevención de crímenes le sugiere que combine números con letras mayúsculas y minúsculas, o que utilice una palabra que no se encuentre en el diccionario. Evite el uso de información personal identificable como por ejemplo su número telefónico, fecha de nacimiento o parte de los números de su seguro social

También es buena idea que utilice una contraseña diferente para cada sitio de Internet que usted use.

Mantenga su contraseña en un lugar seguro. No haga que su computadora le "recuerde" sus contraseñas a menos que usted sea la única persona que tenga acceso a su computadora.

CORREO ELECTRÓNICO (*E-MAIL*)

La diferencia principal entre el correo electrónico y la antigua forma de correo es la privacidad. Piense en el correo electrónico como en una postal en lugar de una carta sellada. Su correo electrónico puede ser interceptado, sea intencionalmente o sin intención en muchos puntos a lo largo de su camino. Por lo tanto, aunque el correo electrónico es una buena forma de estar en contacto, podría no ser una buena forma de enviar información confidencial.

Los criminales están utilizando cada vez más el correo electrónico como una herramienta para realizar fraudes. Algunas de las formas más comunes de estafa son:

1. Estafa de avance de dinero
2. Estafa verificación o "*phishing*"
3. Estafa de lotería internacional

Estafa de avance de dinero

Las estafas de avance de dinero incluyen solicitudes de su información de cuenta bancaria personal o solicitudes para que usted pague dinero por adelantado por concepto de impuestos, honorarios de abofado y otros costos de transacción para poder recibir un beneficio o dinero. Las estafas de avance de dinero incluyen:

1. Desembolso de dinero de testamentos
2. Contracción de fraude
3. Transacciones de bienes raíces
4. Conversión de moneda
5. Transferencia de fondos
6. Venta de petróleo crudo a precios por debajo del mercado.

Un ejemplo común es la “Estafa de Nigeria”. En esta estafa, usted recibirá una solicitud urgente para ayudar a alguien a sacar su dinero de Nigeria (o de otro país). Usted puede recibir documentos que parecen oficiales para respaldar la solicitud, declarando que esto es de un representante oficial de un gobierno o agencia extranjera. Estas solicitudes pueden parecer ser dirigidas personalmente a usted, pero de hecho, las envían en correos masivos. Le ofrecerán una gran cantidad de dinero si pueden hacer movimientos de dinero a través de su cuenta bancaria. Por supuesto, le pedirán el número de su cuenta. Si lo obtienen, vaciarán su cuenta. También le pueden pedir que pague impuestos, honorarios de abogados y otros costos de transacciones por adelantado para “transferir” el dinero a su cuenta.

Si recibe correos electrónicos (o faxes o cartas) similares a alguna de estas estafas:

1. No responda.

2. Destruya o elimine el correo electrónico, fax o carta.

3. Si ha sido víctima de esta estafa, es decir, si usted ha dado su número de cuenta bancaria u otra información de identificación personal o si ha perdido dinero – notifique al Servicio Secreto de los Estados Unidos.

Escriba a: US Secret Service, Financial Crimes Division 245 Murray Drive, Building 410, Washington, DC 20223. Los reclamos por correo electrónico los puede enviar al Servicio secreto (*Secret Service*) a: 419.fcd@usss.treas.gov Al contactar al Servicio Secreto, asegúrese de incluir una copia del correo electrónico original. También puede llamar a la oficina nacional al 202-406-5708 o a la oficina de Boise al 208-334-1403.

Otro ejemplo de estafas de avance de dinero incluye un pago de más en una compra.

Usted se puede convertir en blanco de esta estafa si está vendiendo un objeto a través de la Internet. El "comprador" le enviará "equivocadamente" un cheque por más dinero del precio de compra y le pedirá que le envíe la diferencia. El problema es que el cheque que el "comprador" le envía es falso. Usted perderá su dinero si envía de regreso la cantidad del cheque falso.

Para evitar se víctima de una estafa por pago de más en una compra, usted debe:

1. Confirmar el nombre, la dirección y el teléfono del comprador.

2. Negarse a aceptar un cheque por más de su precio de venta. Si el comprador envía un cheque por más de la cantidad adeudada, devuelva el cheque

y pida que le envíe un cheque por la cantidad correcta. No envíe la mercancía hasta que reciba la cantidad correcta.

3. Considere una fuente alternativa de pago como un servicio de entrega de dinero en depósito o un servicio de pago en línea. Asegúrese de verificar que el servicio de entrega de dinero en depósito o el servicio de pago en línea sea legítimo al revisar su sitio de Internet; revise sus políticas y términos y condiciones; llame a su línea de servicio al cliente; y averigüe con la *Better Business Bureau* o con la Unidad de protección al consumidor del Fiscal general para saber si existe alguna queja o demanda en contra de dicho servicio.

4. No devuelva dinero al comprador.

Estafa de verificación o "*Phishing*"

Si usted es blanco de esta estafa, recibirá un correo electrónico o un mensaje que aparece de pronto, que parece ser de una compañía confiable. Estos correos electrónicos y mensajes con frecuencia contienen gráficos a color y lucen tal como el sitio Internet de la compañía.

El correo electrónico o mensaje indica que la compañía necesita verificar la información de sus registros y le solicitará que dé su número de tarjeta de crédito, el número de identificación personal (*PIN*) del cajero

automático, el número de seguro social y /u otra información confidencial. Esta estafa también se conoce como "*phishing*".

La Oficina del Fiscal General ha visto correos electrónicos fraudulentos que parecen provenir de compañías bastante conocidas como *PayPal*, *E-Bay*, y *MBNA*, una de las principales compañías de tarjetas de crédito. Estos correos electrónicos son fraudulentos y no son de dichas compañías. El remitente está simplemente tratando de obtener información que podría usar para robar su identidad o su dinero.

Las compañías con las que usted hace negocios ya tengan la información que necesitan. Las compañías legítimas no lo contactarán a través del correo electrónico para verificar la información que usted ya les ha dado.

Si usted recibe correos electrónicos (o faxes, cartas o llamadas telefónicas) similares a esta estafa:

1. NUNCA PROPORCIONE LA INFORMACIÓN QUE LE SOLICITAN.

2. Encuentre el correo electrónico de la compañía real y reenvíe el mensaje al departamento de seguridad o fraudes de la compañía. O llame a la compañía a través de un número telefónico que usted esté seguro que es el real.

3. Borre el correo de su computadora. No dé clic en ningún enlace de un correo electrónico sospechoso. Ingrese en las cuentas del sitio de Internet al abrir una ventana nueva del navegador y escribir la dirección URL del sitio de Internet directamente en la barra de direcciones. No "copie y pegue" el enlace URL del mensaje a su barra de direcciones.

4. Utilice solo sitios de Internet seguros para proporcionar información personal o confidencial. Busque el candado  o el icono de la llave  en la parte inferior de su navegador y un URL con una dirección que comienza con "https".

5. Revise los extractos de su tarjeta de crédito y su cuenta bancaria con regularidad para determinar si existe algún cobro no autorizado.

6. Mantenga el software o programa anti-virus actualizado. Algunos correos electrónicos *phishing* contiene virus. Considere la opción de instalar protección *firewall*.

Usted puede reportar el *phishing* ante la *Federal Trade Commission* (FTC) (Comisión federal de comercio). Remita el correo electrónico a *spam*@uce.gov. Si usted cree que ha sido perjudicado (si ha perdido dinero, le han robado su identidad, etc.), por medio del "*phishing*,

usted puede presentar una queja ante la *FTC* en: www.ftc.gov.

Estafa de lotería internacional

Otra estafa común es la estafa de lotería internacional. Esta estafa utiliza el correo electrónico, el correo directo y el teléfono para tentarlo a usted a que compre oportunidades en loterías internacionales. Al enviar dinero para comprar un boleto de lotería, muchos operadores de estafas no compran los tiquetes prometidos. En vez de esto, simplemente se guardan el dinero para ellos. Otros operadores compran algunos boletos y se quedan con los ganadores para ellos. Los operadores con frecuencia hacen retiros no autorizados de su cuenta bancaria o hacen cargos no autorizados a su tarjeta de crédito.

Si usted compra un boleto a uno de estos operadores de estafas, existe una gran probabilidad de que coloquen su nombre en una lista de víctimas potenciales y la vendan a telemercaderistas fraudulentos y a otros estafadores quienes tratarán de venderle otras ofertas falsas de loterías y de "oportunidades de inversión".

Si usted recibe una solicitación para comprar boletos de lotería internacional:

1. No responda a la solicitación.

2. Si la solicitación es por teléfono, presente una queja ante la Unidad de Protección al Consumidor del Fiscal General.

3. Si la solicitación es por correo directo, entregue la carta al jefe de la oficina de correos local.

4. Si la solicitación es por correo electrónico, borre el correo electrónico.

"*Spam*" Correo no deseado

"*Spam*" es la versión de correo electrónico del correo basura: mensajes de correo electrónico no deseado de personas que usted no conoce y que buscan venderle un producto o servicio. Aquellos que envían el correo no deseado (*spammers*), obtienen su dirección de correo electrónico de lugares como sitios de Internet, salas de chat, directorios de miembros y anuncios de grupos de discusión.

Para reducir la cantidad de correo no deseado que usted recibe, usted debe:

1. Considerar tener dos direcciones de correo electrónico. Una dirección de correo electrónico la puede utilizar para mensajes personales y la otra para grupos de discusión y otros propósitos. O, una dirección la puede utilizar como correo electrónico "permanente" y la otra como "desechable".

2. Revise las políticas de privacidad antes de proporcionar su dirección de correo electrónico a un sitio de Internet. Algunos sitios de Internet le permitirán la opción de "decidir no" recibir ofertas o correos electrónicos de otros negocios o de evitar que vendan su dirección de correo a otros negocios.

3. Utilice un filtro de correo electrónico. Su cuenta de correo electrónico puede tener una herramienta para filtrar el correo potencial no deseado o un método para canalizar dichos mensajes no deseados a una carpeta de correo electrónico al por mayor. (*bulk e-mail*).

La *Federal "CAN-SPAM" Act* del año 2003 obliga a los *spammers* (quienes envían el correo electrónico no deseado) a brindarle la opción de "decidir no" recibir correos electrónicos futuros. Sin embargo, muchas personas reportan que reciben correos electrónicos adicionales de otros *spammers* después de que piden ser retirados de la lista del *spammer*. Usted puede reportar a los *spammers* que no cumplen con su solicitud de "no recibir" mensajes ante la *Federal Trade Commission* (FTC) al completar un formato de quejas en www.ftc.gov.

Usted también puede reenviar los mensajes no deseados o engañosos a la FTC a *spam*@ftc.gov o quejarse ante el proveedor de servicio de Internet del *spammer*. Asegúrese de incluir una copia de la

información del mensaje y del encabezado y diga que usted se está quejando del correo no deseado.

SEGURIDAD INFANTIL

La Internet ofrece grandes oportunidades educativas y de entretenimiento para los niños. Pero también ofrece un gran peligro, en especial de parte de los predadores sexuales.

Debido a la naturaleza de ser confiados, los niños son particularmente vulnerables en los "*chat rooms*" (salas de charlas) de Internet. Los predadores infantiles lo saben y con frecuencia se hacen pasar como niños para ganar la confianza y confidencialidad de una víctima potencial.

En Idaho han existido casos en los que un niño ha sido atraído con engaños para encontrarse con un "amigo que conoció en línea" y que resulta ser un adulto y un ofensor o delincuente sexual.

A continuación aparecen unos consejos de seguridad en la Internet para padres e hijos:

1. Comunicación. Hable con sus hijos acerca de los riesgos potenciales de la Internet. Haga que le muestren con frecuencia los lugares de Internet que visitan. Conozca los amigos en línea de la misma manera que lo haría con los amigos que conocen normalmente.

2. Mantenga la computadora en una sala central. Resulta más difícil mantener un secreto cuando los padres pueden ver con frecuencia lo que sus hijos hacen en línea.

3. Utilice los controles de los padres y / o el software de bloqueo. La mayoría de proveedores de servicios de Internet (*ISP*) ofrecen diferentes niveles de controles de los padres que bloquean el acceso a ciertos sitios orientados o creados para adultos. También pueden ser efectivos muchos de los paquetes de software que hay en el mercado.

4. Revise los sitios visitados por sus hijos al revisar los archivos del historial de su navegador memoria caché.

5. Mantenga acceso a la cuenta de sus hijos y de vez en cuando revíseles el correo electrónico. Al principio puede sentir que está invadiendo la privacidad de su hijo, pero píenselo de otra manera. Si su hijo recibe cartas o llamadas telefónicas de un extraño, le preguntaría ¿quién es esa persona?

6. Enséñele a sus hijos que no deben proveer ninguna información acerca de sí mismos. Los predadores pueden utilizar aparentemente información insignificante (por ejemplo *hobbies* o pasatiempos, colegio, edad) para identificar y localizar al niño.

7. Reporte las actividades no apropiadas en línea. Notifique inmediatamente a la policía si un contacto en línea trata de establecer una cita con su hijo.

8. No permita que sus hijos usen las salas de charlas. Inclusive las salas de charlas para “niños” que parecen seguras pueden ser peligrosas.

El *National Center for Missing and Exploited Children* (Centro nacional para los niños perdidos o explotados) ha creado un programa de seguridad en Internet muy útil, informativo y divertido, para los padres y los hijos. Lo encontrará en www.netsmartz.org.

PRIVACIDAD

Algunos sitios de Internet pueden compartir su información con los afiliados. Además, pueden vender su información personal. Antes de proporcionar la información en un sitio de Internet, decida qué tipo de información desea mantener privada y que tipo de información desea entregar.

Si le preocupa la privacidad, tenga en cuenta los siguientes consejos.

Información personal

Nunca de su número de seguro social o número de licencia de conducir a través de la Internet.

No revele información personal como su dirección, número telefónico o dirección electrónica a menos que haya consultado la política de privacidad de la compañía y que esté seguro de que la compañía tiene buena reputación. Aún así, entérese exactamente de qué información está siendo recolectada y de qué manera la compañía la utilizará. Muchas compañías se han unido con otros afiliados o socios que tienen acceso completo a los archivos de sus clientes.

Enseñe a sus hijos a no dar en línea su información personal o acerca de la familia.

Políticas de privacidad

Muchas compañías publican la política de privacidad en su sitio de Internet. Si no puede localizar la política de privacidad de una compañía, envíe un correo electrónico o una solicitud por escrito para recibir una copia.

Lea la política de privacidad cuidadosamente antes de proporcionar al sitio su información personal. Revise si la compañía transferirá la información personal que usted proporcione a los afiliados o a otros negocios u organizaciones.

Seguridad del sitio

Antes de realizar alguna transacción en línea, verifique que el sitio de Internet de la compañía sea seguro. Un sitio seguro significa que la compañía ha tomado las precauciones necesarias para asegurarse de que otras

personas no puedan interceptar la información. Usted **siempre** verá un candado  o un icono de una llave  en la esquina inferior de la pantalla cuando un sitio es seguro.

Asegúrese de que su navegador tenga la capacidad más actualizada de codificación. También, busque la expresión: “https:” en el URL.

Cookies

Las “*Cookies*” son partes de datos que un sitio de Internet coloca en el disco duro de su computadora. Las *cookies* se originan de los sitios que usted visita. En efecto, las *cookies* registran de manera digital sus entradas y salidas.

Las *cookies* sólo las puede leer el servidor de red que las originó. Otros servidores de red no pueden interceptarlas.

Las *cookies* desempeñan muchas funciones, por ejemplo, sirven como herramientas de navegación o como medio para buscar en Internet. Las *cookies* también guardan el registro de los bienes que usted intenta comprar pero que deja de lado cuando termina una transacción en un sitio de Internet. Las *cookies* pueden reunir y transferir una gran cantidad de información acerca de usted y sus intereses cada vez que está en línea, inclusive cuando usted paga la cuenta o se desconecta.

Tanto el navegador *Netscape Navigator* como el Microsoft le permiten bloquear las *cookies* o le avisan antes de que una *cookie* se descargue a su computadora. Sin embargo, al impedirlo, usted puede reducir o incluso eliminar las opciones de navegación en muchos sitios de Internet.

Para mayor información acerca de las *cookies* y cómo eliminar las *cookies* de su navegador completamente, visite www.cookiecentral.com.

Pharming

"*Pharming*" implica la redirección de un usuario de Internet de un sitio comercial legítimo de Internet a un sitio de Internet falso. Los "*pharmers*" crean sitios falsos y enlazan a usuarios de sitios de Internet legítimos al alterar el sistema de nombre del dominio o al transmitir un virus.

El sitio falso se verá como el sitio de Internet legítimo. Al ingresar su nombre para conectarse o su identificación y contraseña, los "*pharmers*" obtienen la información para su uso. Esto puede ocurrir incluso cuando usted escribe el URL correcto.

Usted puede seguir algunas indicaciones para evitar ser víctima de *pharming*:

1. Mantenga actualizado el software o programa de anti-virus.

2. Considere la opción de instalar software anti-*spyware* y *firewalls*.

3. Tenga cuidado al ingresar información personal o confidencial al sitio de Internet. Asegúrese de buscar el candado  o el icono de la llave  en la parte inferior de su navegador.

4. Revise cuidadosamente los sitios de Internet. Si el sitio de Internet ha cambiado desde su última visita, desconfíe de este. Si tiene alguna duda acerca del sitio de Internet, no lo use.

Spyware

Spyware es el software que se instala en su computadora sin su consentimiento. *Spyware* controla el uso de su computadora sin que usted lo sepa. También se le llama "*adware*". *Spyware* es usado con frecuencia para enviarle a usted ventanas con anuncios o propagandas, para dirigirlo a algunos sitios de Internet, para controlar la forma como usted navega en la Internet e incluso para grabar lo que usted teclea. *Spyware* puede conducir al robo de identidad.

Es posible que usted tenga *spyware* instalado en su computador si experimenta problemas como numerosas ventanas que aparecen con propagandas; si un navegador lo lleva a sitios diferentes de los que usted escribió en la barra de direcciones; si con frecuencia o de forma repetitiva se cambia su página de inicio; si

aparecen barras de herramientas o íconos en la parte inferior de la pantalla de su computadora; si hay teclas que ya no funcionan; si aparecen mensajes de error aleatoriamente, o si el desempeño es lento al abrir programas y guardar archivos.

Para evitar la instalación de *spyware*:

1. Mantenga actualizados su sistema operativo y el software de su navegador.

2. No baje software de sitios que no conozca y en los que no confíe.

3. No instale software sin saber exactamente lo que es. Lea el acuerdo de permiso para el usuario final antes de instalar software.

4. Ajuste el controlador de seguridad de su navegador en un nivel alto y manténgalo actualizado.

5. No de clic en enlaces dentro de ventanas que aparezcan con propagandas. Cierre dichas ventanas tan sólo dando un clic en el icono de la "x" en la barra de título.

6. No de clic en enlaces de correo no deseado que ofrezcan software "anti-*spyware*". Muchos de estos son fraudulentos y en realidad instalan *spyware* en su computadora.

7. Considere la posibilidad de instalar un *firewall*.

OPORTUNIDADES DE NEGOCIOS EN LÍNEA

La Internet también ofrece muchas oportunidades de negocios. Si encuentra alguna que le interese, asegúrese de investigar a fondo la compañía antes de inscribirse.

La comisión federal de mercadeo (sigla en Inglés *FTC*) le sugiere que:

- Entienda que los "asesores" en los seminarios están usualmente en los negocios para venderle una oportunidad de negocio más que para enseñarle la información básica acerca de la Internet. En algunos casos podrían buscar explotar su falta de experiencia en computadoras o con la Internet.

- Investigue todas las declaraciones o promesas de ganancias. Hable con otras personas que hayan comprado la oportunidad para ver si su experiencia está de acuerdo con lo que propone la compañía.

- Solicite ver las propuestas y promesas de la compañía por escrito.

- Pida un documento de revelación. La Ley de Franquicia de la *FTC* exige que la mayoría de oportunidades de negocios tengan a disposición un documento de revelación. El documento de

revelación debe contener información detallada que le ayudará a comparar entre un negocio y otro.

- Pregunte por el negocio en la oficina local de *Better Business Bureau* y/o a la agencia de protección al consumidor en el estado donde el negocio está ubicado. Su consulta podría mostrarle si han presentado algunas quejas concernientes al negocio.

Estafas de negocios en Internet

La Internet es usada para perpetrar una variedad de estafas. Los consumidores se quejan de algunos de los siguientes puntos que aparecen en Internet:

- Subastas: Usted recibe un objeto que no es como se suponía, de menor valor a lo prometido, o no recibe nada en absoluto. Algunas veces los vendedores no hacen el envío de forma oportuna o no dan toda la información relevante acerca del producto o términos de venta.

- Servicios de acceso a Internet: usted cobra un cheque que recibió de un negocio y luego queda amarrado a un contrato a largo plazo para tener acceso a Internet u otro servicio de Internet, con castigos legales si cancela el contrato o si lo da por terminado antes de tiempo.

- Ofertas para trabajar en casa: a usted le ofrecen la oportunidad de ganar “muchos dólares” al trabajar en casa o al comenzar un negocio nuevo. De hecho, usted trabajará muchas horas sin que le paguen y es posible que usted tenga que pagar dinero por adelantado.

- Avances de préstamos: a usted le ofrecen préstamos si usted paga cierta cantidad, sin importar su historia crediticia pasada. Estas ofertas con frecuencia son una manera de recolectar dinero sin que en realidad le proporcionen ningún préstamo legítimo.

- Ventas de mercancías en general: usted no recibe la mercancía, no es el valor o calidad de la mercancía prometida o a usted le cobran dinero extra.

- Ofertas de viaje: a usted le ofrecen viajes de lujo por precios de ofertas y recibe alojamiento y servicios de baja calidad o no recibe nada, o le cobran dinero extra.

- Pirámides, mercadeo a multi-nivel y cartas de cadenas: A usted le ofrecen la oportunidad de hacer dinero al vender productos y servicios y atraer a otras personas hacia el programa. Ni usted ni las personas que trae al programa ganan ningún dinero. Muchos de estos programas son ilegales.

- Ofertas de pérdidas de peso: A usted le ofrecen un tratamiento “milagroso”, pero en vez de este le venden productos inútiles e incluso algunas veces peligrosos.

- Ofertas de reparación de sus registros de crédito: A usted le ofrecen la oportunidad de borrar la información negativa de sus registros de crédito. Estas ofertas son falsas.

- Ofertas de entretenimiento para adultos: A usted le ofrecen la oportunidad de ver imágenes para adultos “gratis” su comparte el número de tarjeta de crédito para probar que usted es mayor de 18 años de edad. O a usted le ofrecen acceso “gratis” a material para adultos al descargar un programa de visualización o de marcado para la computadora. Lo que debe esperar es que le llegue un cobro en su tarjeta de crédito. Luego puede recibir cobros de llamadas de larga distancia internacional en su factura de teléfono por marcado internacional a través del módem.

- Engaño a través de sitios de Internet: A usted le ofrecen acceso gratis a un sitio de Internet por un período de prueba y luego le aparecen cobros en su factura de teléfono o recibe facturas de los sitios de Internet.

- Oportunidades de inversión: A usted le ofrecerán una “oportunidad invirtiendo muy poco” o le prometen grandes ganancias en corto tiempo. A usted le cobrarán dinero por adelantado o no recibirá ninguna inversión legítima. Sea cauteloso con las inversiones que aseguran que están aprobadas por la “IRS” o que no cobran impuestos y son confidenciales.

VIRUS DE COMPUTADORA

¿Qué es un virus?

Un virus es un programa o archivo colocado en su computadora sin su consentimiento. Su propósito es dañar archivos y alterar su computadora.

¿Cómo se infecta una computadora con un virus?

La mayoría de virus se propagan por medio de archivos adjuntos enviados a través del correo electrónico o en un disquete, CD, DVD o una memoria removible. Cuando usa un archivo infectado en su computadora, el virus se copia a sí mismo en su disco duro. Algunos virus atacan y causan problemas inmediatamente. Otros permanecen inactivos hasta que se usa un programa específico o hasta después de cierta fecha.

Los virus se propagan muy rápidamente. Si descubre que su computadora ha sido infectada, debe asumir que cada archivo y computadora que haya usado también esta infectada. Una falla al explorar y desinfectar cada

disco y computadora puede ser garantía de que el virus reinfectará su computadora o su red nuevamente.

¿Cómo se elimina un virus?

Por lo general, los virus se pueden eliminar solamente usando un software anti-virus o formateando el disco duro infectado. Si sospecha que su computadora esta infectada con un virus, necesitará buscar un software anti-virus y comprar el paquete adecuado. Algunas marcas conocidas son *Norton, McAfee y Kapersky*.

Una vez que su software anti-virus sea instalado, existe la opción de restaurar o reparar la información dañada y eliminar algunos archivos dañinos o peligrosos que estaban guardados en su computadora. Sin embargo, existe la posibilidad de que haya perdido información que no se puede recuperar. Usted puede reducir este riesgo haciendo frecuentemente "*back-ups*" (copias de resguardo) de su información personal.

Mantenimiento preventivo

- Asegúrese que todas las computadoras tengan instalado el software anti-virus.

- Actualice por lo menos una vez al mes los archivos de definición de virus desde el sitio de Internet del fabricante del software anti-virus.

- Revise los archivos adjuntos de correo electrónico antes de abrirlos y revise los disquetes antes de usarlos en su computadora. No baje archivos que le han sido enviado por personas que usted no conoce.

- Haga "*back ups*" (copias) de su información personal con frecuencia y con un horario regular. No haga las copias en su disco duro principal hágalas en Cd's grabables (CD-R), *zip drives* (unidades Zip) o disquetes.

APÉNDICE A

Recursos en línea

Encontrará más información acerca de la seguridad en Internet en estos sitios de Internet.

www.ag.idaho.gov

Esta publicación está disponible en el sitio Internet del Fiscal General. El sitio del Fiscal General también contiene publicaciones acerca de otros temas de protección al consumidor.

www.fraud.org

La liga nacional de consumidores (*National Consumers League*) brinda consejo acerca de la Internet y del fraude en Internet. Usted puede reportar las probables estafas a través de un formato en línea.

www.netsmartz.org

El Centro nacional para los niños perdidos y explotados (*National Center for Missing & Exploited Children*) proporciona información acerca de la seguridad infantil para los padres y los hijos.

www.consumer.gov

El sitio Internet de la agencia federal proporciona publicaciones e información al consumidor.

www.pueblo.gsa.gov

El manual de recursos del consumidor (*Consumer's Resource Handbook*) disponible en este sitio de Internet del gobierno federal, enumera las agencias locales, estatales y federales, las principales asociaciones de mercadeo y los grupos de consumidores.

www.bbbonline.org

El programa de confiabilidad del *Better Business Bureau* para comerciantes que participan en línea, los conecta con el sitio central del *BBB* para reportes acerca de negocios e información acerca de cómo contactar un *BBB* específico a lo largo de los Estados Unidos.

www.ftc.gov

La Comisión federal de mercadeo (*Federal Trade Commission*) ofrece panfletos o folletos en línea relacionados con las compras en Internet, estafas de correo electrónico o de Internet, oportunidades de negocios en línea y temas adicionales de interés para el consumidor. La *FTC* también ofrece un formulario para presentar reclamos en línea para los consumidores que enfrenten problemas dentro del mundo mercantil.

APÉNDICE B

Glosario

La Internet tiene su propia terminología. A continuación aparecen algunos términos claves.

Adware – *Adware* es software que se instala en su computadora sin su consentimiento. *Adware* controla el uso de su computadora sin que usted lo sepa. También se llama "*spyware*".

Attachment (archivo adjunto)– Es un archivo que se envía junto con el mensaje de correo electrónico.

Browser (navegador)– Un navegador es el programa que solicita documentos de los servidores y los muestra en su pantalla. Lo más seguro es que el programa que usted está utilizando en su casa sea un navegador de red. Entre los navegadores populares están: *Netscape Navigator*, *Lynx*, y *Microsoft Internet Explorer*.

Cookie – Pequeños archivos que algunos sitios de Internet que usted visita, ubican en el disco duro de su computadora.

Download (Descargar)– Copiar archivos de la Internet a su computadora.

E-mail o electronic mail (correo electrónico)– mensajes, similares a cartas que se envían o reciben a

través de la Internet. Los mensajes se pueden dirigir a una persona o a un grupo de personas.

Encryption (Codificación)– Un algoritmo utilizado para convertir o codificar datos que hace que los datos sólo los pueda leer el receptor o destinatario. Con frecuencia los sitios de comercio electrónico utilizan la codificación para asegurar los datos de las tarjetas de crédito. Los sitos de Internet seguros utilizan la codificación.

Hyperlink (hipervínculo)– Una conexión electrónica que automáticamente lo lleva de un sitio de Internet a otro. Por ejemplo, el sitio de Internet del Fiscal General le proporciona un hipervínculo a la página de la Unidad de Protección al Consumidor.

Internet commerce (e-commerce) (comercio electrónico) – Compra y venta de bienes y servicios a través de la Internet. Las transacciones se realizan entre los negocios y los consumidores por medio de una red de computadoras.

Módem – Un dispositivo de hardware que utiliza líneas de cable o teléfono para conectar su computadora a la Internet o permitir que usted se comunique con otras computadoras.

Pharming – "*Pharming*" implica la redirección de un usuario de Internet de un sitio comercial legítimo a un sitio falso. Los "*pharmers*" crean sitios falsos y enlazan

a usuarios de sitios de Internet legítimos al alterar el sistema de nombre del dominio o al transmitir un virus.

Phishing – "Phishing" es una estafa que pretende obtener sus contraseñas y otra información personal y confidencial que puede ser usada para robar su identidad. El "*Phishing*" lo realizan al enviar un correo electrónico fraudulento que parece venir de un negocio legítimo. Usualmente el correo electrónico contiene un enlace a un sitio de Internet falso (pero que se ve como si fuera legítimo). Si usted ingresa en el sitio fraudulento, los "*phishers*" capturarán su identificación y contraseña de usuario lo que les permitirá tener acceso a su cuenta.

Search engine (motor de búsqueda o buscador)– Un programa que busca palabras claves específicas o frases a través de la Internet y que proporciona una lista de documentos que contienen las palabras claves o las frases. Google, Excite, y Yahoo son algunos de los buscadores más reconocidos.

Spam – El "*spam*" es la versión de correo electrónico del correo del correo basura: mensajes de correo electrónico no deseado de personas que usted no conoce y que buscan venderle un producto o servicio.

Spyware – el "*spyware*" es un software que se instala en su computadora sin su consentimiento. *Spyware* controla el uso de su computadora sin que usted lo sepa. También se llama "*adware*".

URL – *Uniform Resource Locator*. (Localizador de recursos uniformes) Esta es la dirección de un sitio de Internet específico. Usted puede digitar el URL en su computadora para que lo lleve directamente a ese sitio en la Internet. Por ejemplo, www.ag.idaho.gov es la dirección URL de la Oficina del Fiscal General.

Virus – Un archivo colocado en su computadora que puede dañar o alterar su computadora.

Website (Sitio de Internet)– Un destino de Internet donde usted puede buscar o consultar información.

Los fondos para pagar esta publicación provinieron de subvenciones que obtuvo la Unidad de Protección al Consumidor del Fiscal General. Los contribuyentes de impuestos no pagan por los esfuerzos de educación al consumidor del Fiscal General tales como la publicación de este folleto.

La Unidad de Protección al Consumidor hace cumplir las leyes de protección al consumidor de Idaho, brinda información al público de asuntos del consumidor y ofrece un proceso de mediación de información para quejas particulares de consumidores.

Si usted tiene un problema o una pregunta como consumidor, favor de llamar al 208-334-2424 ó gratis en Idaho al 1-800-432-3545. Están disponibles el acceso TDD y los servicios de interpretación Language Line. La página de Internet del Fiscal General está disponible al www.ag.idaho.gov.