Oficina del
Fiscal General

Seguridad en Internet

(Internet Safety)

LAWRENCE WASDEN
FISCAL GENERAL
700 West Jefferson Street
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 DEL CONSUMIDOR

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, las redes sociales, navegar y hacer negocios en línea.

Uno de los mayores 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. Es muy importante que use siempre la versión más actualizada de su navegador y que revise regularmente si hay actualizaciones de seguridad y de programas.

Si usted no tiene un navegador seguro, hay muchos de donde elegir. Los dos navegadores más comunes son Microsoft

Internet Explorer y Mozilla Firefox. Los dos navegadores los puede descargar gratis desde la Internet.

Al comprar en línea, también es importante que compre desde un sitio seguro. Para mayor información, consulte la sección "seguridad de los sitios de Internet".

Compre con compañías que 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 sede del negocio para averiguar que clase de antecedentes tiene el negocio. Averigüe con la Secretaría de Estado para ver si el negocio está registrado. 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.). Si es posible, compare la descripción con un modelo físico real del mismo objeto.

Revise la letra pequeña y busque palabras como "restaurado", "liquidación", "defectuoso", "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.

Tenga precaución de las ofertas "de prueba gratuitas". Al solicitar una muestra de prueba, usted puede estar iniciando una obligación a largo plazo, incluyendo envíos mensuales de productos adicionales y cargos a su cuenta. No de el número de su tarjeta de crédito ni información de su cuenta bancaria para recibir una muestra "de prueba gratuita". Si en realidad es una oferta gratuita, el negocio no necesita la información de su cuenta.

Sitios de subastas en Internet

Comprar en un sitio de subastas no lo protege automáticamente del fraude. De hecho, algunos sitios de subasta en Internet pueden ser completamente fraudulentos. Compre únicamente en sitios que conozca o que pueda verificar que son legítimos.

Al comprar en un sitio de subastas, siempre debe entender y seguir las guías del sitio. Salir del sitio para pagar por una compra lo pone en mayor riesgo de fraude y de perder su dinero. Algunos vendedores o compradores ofrecerán negociar con usted directamente a través de su correo electrónico, por ejemplo afirmando que su oferta ganó una opción de "segunda oportunidad". Esta es una táctica usada

con frecuencia por estafadores como un intento de alejarlo a usted de las garantías de protección del sitio.

Sea especialmente precavido ante los compradores y vendedores fuera de los Estados Unidos. Gran parte de los fraudes reportados en estos sitios ocurren con transacciones extranjeras. Si usted pierde dinero en una estafa por Internet, usted prácticamente no tendrá la oportunidad de recuperarlo, especialmente si el vendedor está en un país diferente.

Si usted tiene una queja o reclamo por una compra en un sitio de subastas, contacte al vendedor a través del sistema del sitio de subastas. No se comunique "fuera del sitio" ni por correo electrónico. Si no está satisfecho con la respuesta del vendedor, utilice el proceso de reclamación del sitio. Asegúrese de actuar dentro del margen de tiempo permitido por el sitio. No permita que el vendedor se retrase hasta que haya pasado la fecha límite de la reclamación. Si usted paga con tarjeta de crédito, es posible que también pueda reclamar cargos con su compañía de tarjeta de crédito.

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 de 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 débito, existen protecciones por pagos no autorizados bajo la *federal Electronic Fund Transfer Act*. Para mayor información sobre estas leyes, comuníquese con la División 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:

- Estafas de avance de dinero,
- "phishing" o estafas de verificación, y
- Estafas de lotería internacional.

Estafas 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:

- Desembolso de dinero de testamentos,
- Contracción de fraude,
- Transacciones de bienes raíces,
- conversión de moneda,
- transferencia de fondos,
- venta de petróleo crudo a precios por debajo del mercado y

- premios o recompensas monetarias.

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 o transmisiones masivas. 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 la oficina más cercana del Servicio Secreto de los Estados Unidos. El número telefónico de la oficina local en Idaho es (208) 334-1403.

Otro ejemplo de estafas de avance de dinero incluye un pago de más por 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 sobrante 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 número telefónico 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. No envíe el dinero sobrante del cheque al comprador.
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 División de protección al consumidor del Fiscal general para saber si existe alguna queja o demanda en contra de dicho servicio.

"Phishing" o estafas de verificación

Si usted es blanco de esta estafa, recibirá un correo electrónico o un mensaje que aparece de pronto, o mensaje de texto en su teléfono celular 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 y mensajes de texto fraudulentos que parecen provenir de compañías bastante conocidas como *PayPal, E-Bay,* y compañías principales de tarjetas de crédito y bancos comunitarios. 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 tienen 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, mensajes de texto 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 electrónico o mensaje de texto. 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. Esta información se utiliza con propósitos de hacer cumplir la ley contra personas que envían correos engañosos. Si cree que ha sido perjudicado (si ha perdido dinero, le han robado su identidad, etc.) por medio del "phising", usted puede presentar una queja ante la FTC en: www.ftccomplaintassistant.gov.

Estafas de lotería internacional

Las estafas de lotería internacional utilizan los correos electrónicos, correo directo y el teléfono para tentarlo a comprar 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 División 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.ftccomplaintassistant.gov.

Usted también puede reenviar los mensajes no deseados o engañosos a la FTC a spam@uce.gov o quejarse ante el proveedor del servicio de Internet del *spammer*. Esta información se utiliza con propósitos de hacer cumplir la ley contra las personas que envían correos engañosos. Asegúrese de incluir una copia del la información del mensaje y del encabezado y diga que usted se está quejando por el correo no deseado.

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 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.

La mayoría de los navegadores le permiten bloquear las *cookies* o le avisan cuando una *cookie* se descarga en 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 eliminarlas 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 da los siguientes consejos:

- 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

Los consumidores se quejan de algunos de los siguientes asuntos relacionados con 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 rescate de ejecución hipotecaria: A usted le ofrecen la oportunidad de salvar su casa de la ejecución hipotecaria al pagar una cantidad de dinero por adelantado. Muchas de estas compañías reciben su dinero y no dan ninguna modificación de préstamo ni proporcionan ningún servicio para salvar su casa de la ejecución hipotecaria.

- 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

¿Que 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 y funcionando.

- Actualice por lo menos una vez a la semana 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 medios removibles 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 CDs o DVDs, en un disco duro externo u otro medio de almacenamiento removible.

SEGURIDAD INFANTIL

PELIGROS EN LÍNEA PARA NIÑOS - INTRODUCCIÓN

Hasta hace unos pocos años, "entrar en línea" significaba sentarse frente a una computadora de escritorio y conectarse a la Internet. Hoy en día, existen computadores portátiles inalámbricos, teléfonos celulares con Internet, capacidad de enviar fotos y texto, Blackberries y aparatos similares. Incluso los sistemas de juego como PlayStation, Xbox y Wii conectan personas en lugares distantes con texto, voz y comunicación de video interactivo. ¡La seguridad en línea ya no está limitada a las computadoras!

Con todos los beneficios que brinda el mundo en línea, también puede plantear peligros significativos para los niños.

Estos peligros por lo general se enmarcan en las siguientes tres categorías:

1. Victimización sexual

2. Exposición a la pornografía y/o violencia
3. Ciberacoso

Victimización sexual

Debido a su naturaleza confiada, los niños son particularmente vulnerables en las "salas de plática" y en los sitios de redes sociales de Internet. Los depredadores sexuales saben esto y con frecuencia se hacen pasar por niños para ganarse la confianza de una víctima potencial.

Han existido muchos casos en Idaho en los que un niño ha sido atraído con engaños para encontrarse con un "amigo en línea" que resulta ser un adulto y delincuente sexual.

Es peligroso que los niños publiquen información de identificación personal en la Internet puesto que un depredador sexual puede usar esta información para identificar y localizar a un niño para volverlo víctima. Dicha información incluye fotografías, nombre, dirección, edad, escuela, actividades extra curriculares, nombres y ocupaciones de los padres y cualquier otra información que un depredador podría utilizar para identificar y localizar a un niño.

La naturaleza anónima de la Internet se suma a los peligros para los niños. La gente puede pretender ser alguien en línea y uno casi nunca puede estar seguro de que la persona con quien se está comunicando es en realidad quien dice ser.

Los depredadores sexuales tratarán de establecer comunicación con una víctima potencial a través del correo electrónico, las salas de plática, los sitios de redes sociales, mensajes de texto e incluso video juegos. Los depredadores esconden su verdadera identidad, con frecuencia pretendiendo ser un adulto comprensivo que "entiende" los problemas del niño. Algunas veces ellos conducirán a los

niños a creer que se están comunicando con otro niño. Ellos usan este tipo de tácticas para establecer una relación de confianza con la víctima potencial, un proceso conocido como *"grooming"* (preparar a las víctimas con atención y simpatía). Una vez que se establece la confianza, el depredador intenta encontrarse con el niño en persona. El niño ya no piensa que el depredador es un extraño, sino un amigo que entiende y se preocupa por los problemas del niño, alguien que el niño desea conocer en persona.

Exposición a la pornografía

Algunas veces usted puede encontrarse con pornografía en línea de manera accidental. Puede estar ligada a un correo electrónico o a una ventana emergente o incluso ser enviada a su teléfono celular. Algunos pornógrafos usan deliberadamente nombres de sitios de Internet similares a los sitios que es probable que los niños visiten mientras hacen su tarea. Aunque hace años fue cerrado, una vez existió un sitio pornográfico en Internet llamado "whitehouse.com[1]." El sitio Internet real de la Casa Blanca es "whitehouse.gov."

La exposición a la pornografía no sólo se limita a las computadoras. La pornografía se puede bajar y ser vista en cualquier aparato en línea, como teléfonos celulares y iPods. Es importante que los padres estén enterados que contenido tienen los chicos en sus aparatos móviles.

Ciberacoso

De acuerdo con el *National Crime Prevention Council*, (Consejo Nacional de prevención de crímenes), casi la mitad de todos los adolescentes estadounidenses han sido víctimas del ciberacoso. El ciberacoso ocurre cuando los adolescentes utilizan la Internet, teléfonos celulares u otros aparatos

[1] The current Internet address whitehouse.com is not connected with the former pornographic website.

digitales para enviar o publicar mensajes o imágenes con la intención de herir, humillar o avergonzar a otra persona.

Existen leyes en Idaho que protegen a las víctimas de hostigamiento, intimidación y acoso. Si usted considera que su hijo es víctima de ciberacoso, hable de inmediato con el consejero de la escuela o el policía asignado a la escuela. El ciberacoso puede tener efectos muy serios sobre su hijo, que lo pueden llevar al retraimiento, la depresión e incluso al suicidio.

Señales de advertencia para padres

A continuación aparecen algunas señales de advertencia de que su hijo va camino a tener problemas en línea. Si usted nota alguno de estos comportamientos, debería hablar con su hijo respecto a estos.

- Su hijo cambia o minimiza la pantalla de la computadora cuando usted entra a la habitación.
- Su hijo comienza a pasar mucho más tiempo en línea.
- Su hijo comienza a recibir llamadas telefónicas de personas que usted no conoce.
- Su hijo tiene ropa nueva, CDs u otros objetos regalados por fuentes desconocidas.
- Su hijo se disgusta demasiado si el acceso a Internet está restringido o no está disponible aunque sea por un período corto de tiempo.
- Su hijo está inusualmente retraído o poco comunicativo.

La *Idaho Internet Crimes Against Children Task Force* (Fuerza especial de crímenes en Internet contra niños de Idaho)

La *Idaho Internet Crimes Against Children (ICAC) Task Force* es una coalición a nivel estatal de agencias de interposición de acción judicial y aplicación de la ley federal, estatal y local, enfocada en detener y procesar personas que usan la Internet para explotar niños de manera criminal.

Los crímenes contra niños en Internet son, ante todo, crímenes de explotación sexual de niños. Estos crímenes incluyen distribución de pornografía infantil y uso de la Internet para encontrar niños como objetivos de abuso sexual.

La Idaho ICAC Task Force está comprometida para proteger los niños de Idaho a través de la educación a la comunidad y la identificación, arresto y procesamiento de aquellos que cometen crímenes contra niños en Internet. Para mayor información, visite www.icacidaho.org.

Reporte de crímenes contra niños en Internet

Usted puede ayudar en la lucha contra la explotación de niños al reportar información que considere útil. Puede contactarnos a través de la línea nacional *CyberTipline* en www.cybertipline.com o al llamar gratis al (800) 843-5678.

La información que usted proporcione se enviará a las agencias de aplicación de la ley apropiadas de *ICAC* en Idaho o en cualquier otro lugar de los Estados Unidos.

Guías generales para la seguridad de la computadora

- Participe activamente en el uso de Internet de sus hijos. Enséñeles que deben contarle si se encuentran

algo que los hace sentir incómodos, que los confunde o que sea pornográfico.

- Comuníquese. Hable a si hijo sobre los riesgos potenciales de la Internet. Haga que regularmente le muestren los sitios que visitan. Conozca sus amigos en línea de la misma manera que lo hace con sus amigos normales.
- Reporte la actividad inadecuada en línea. Notifique a la policía local o al sheriff inmediatamente si un contacto en línea trata de acordar un encuentro con su hijo. Usted también debe reportar esto ante la línea nacional CyberTipline en www.cybertipline.com o al llamar gratis al (800) 843-5678.
- Establezca límites. El contrato familiar para la seguridad en Internet es un buen punto de partida. Usted puede imprimirlo del DVD de ProtecTeens o del sitio Internet del Fiscal General. Revíselo con sus hijos, fírmenlo juntos y colóquenlo cerca de la computadora, donde sus hijos recordarán las reglas que acordaron cumplir cada vez que entren en línea.
- Controle el uso de Internet de sus hijos. Conozca los sitios que visitan. Revise los archivos del historial del navegador y memoria caché y decida si los sitios son apropiados para sus hijos.
- Mantenga acceso a las cuentas de sus hijos y de vez en cuando revise el correo electrónico y cualquier sitio de redes sociales que visite su hijo. Si entra a salas de plática o envía mensajes instantáneos, asegúrese de saber con quién está platicando. Revise las listas de amigos y registros de pláticas.
- Ubique las computadoras en línea en un área común de la casa, donde pueda observar frecuentemente el monitor y ver que está viendo su hijo. Los niños no

deben tener computadoras en línea en sus habitaciones.

- Aprenda y use los programas de controles para padres. Puede usarlos para bloquear sitios de Internet inapropiados, limitar la cantidad de tiempo que pasa su hijo en Internet, y controlar la actividad en línea. Encontrará mayor información acerca de programas de control para padres en el DVD de ProtecTeens y en el sitio Internet del Fiscal General.

- Hable con sus hijos sobre la naturaleza anónima de la Internet. Asegúrese de que entienden que cualquier persona puede pretender ser quien quiera en línea y que las personas que conocen en línea pueden no ser quienes dicen ser. Enséñeles a que sólo deben hablar en línea con las personas que conocen en realidad en persona.

- Enseñe a los niños a proteger su verdadera identidad en línea. Por ejemplo, los niños no deberían llamar la atención con el hecho de que son niños. Es una mala idea utilizar un nombre de pantalla que sugiera la edad, como "Jessica14". La información personal se puede utilizar para el robo de identidad. Los ladrones de identidad con frecuencia tienen como objetivo a los niños porque el crimen no se puede descubrir hasta años más tarde, cuando el niño víctima de robo de identidad crezca y trate de comprar un carro u obtener una tarjeta de crédito. Nunca se debe dar a nadie que haya conocido en línea el número de seguro social, los números de cuentas bancarias, los números de tarjetas de crédito o débito, o la fecha de nacimiento o dirección física. No responder a correos electrónicos u otros mensajes que pidan este tipo de información. Simplemente bórrelos.

- Enseñe a los niños que la Internet es el lugar más público del mundo. Si usted publica una foto,

cualquier persona puede verla y nunca la podrá regresar. Inclusive si usted publica en un lugar seguro, la foto puede ser copiada y enviada por correo electrónico o puede ser publicada en otro sitio. Los depredadores pueden buscar fotos de niños que encuentren atractivos y luego tratan de localizar a estos niños. Inclusive las fotos de sitios de noticias, sitios familiares, sitios de escuelas y sitios de clubes pueden ser utilizados erróneamente para hacer daño a los niños.

- Hable con sus hijos del "*sexting*", la práctica de enviar fotos sugestivas o de desnudos a amigos a través del teléfono celular. Asegúrese que entienden que una vez envían una foto, han perdido el control de esta y nunca la pueden recuperar. La persona a la que se la envían puede enviársela a otras personas. Estas fotos pueden terminar en la Internet y causar problemas mayores años más tarde, cuando llegue el momento de conseguir un trabajo o ingresar a la Universidad. Estas fotos también pueden causar problemas hoy en día. Otros niños pueden usarlas para armar chismes o acosar a su hijo. Un niño que envía o posee estas fotos puede ser procesado por pornografía infantil y puede ser que requieran que aparezca registrado como un delincuente sexual de por vida.

- Asegure sus redes inalámbricas. Las personas fuera de su casa pueden acceder a la Internet a través de redes inalámbricas desprotegidas. Pueden bajar pornografía, tener a un niño como objetivo o cometer cualquier otro crimen en Internet. Si el criminal es atrapado, aparecerá que su computadora fue utilizada para cometer estos crímenes. Si usted instala una red inalámbrica, asegúrese de proteger el acceso con contraseña a la red a través de métodos de codificación inalámbrica como WEP, WPA o WPA2.

Cuando esté disponible, marque la casilla "codificar" para protección adicional. Para mayor información acerca de cómo asegurar una red inalámbrica, visite www.icacidaho.org o contacte a su proveedor de servicio de Internet.

PROGRAMAS DE CHAT (PLÁTICA)/ MENSAJERÍA INSTANTÁNEA/TELÉFONOS CELULARES

Salas de plática

Las salas de plática son sitios de Internet que las personas usan para conversar. Las salas de plática pueden ser un lugar peligroso para los niños. Las conversaciones son "en vivo" o "en tiempo real", lo que significa que la comunicación es instantánea. El peligro de una sala de plática es que la persona con quien usted está platicando puede ser o no sincera sobre su identidad. Las conversaciones pueden ser sexualmente ofensivas y violentas. No permita que sus hijos usen las salas de plática. Inclusive las salas de plática que parecen seguras para los "niños" pueden ser peligrosas.

Mensajería instantánea

La mensajería instantánea, también conocida como *IMing*, es una forma común de comunicación instantánea persona a persona. Es un método que los depredadores pueden utilizar para comunicarse con los niños. MS Messenger es un programa de mensajería instantánea popular. Yahoo, Google y otros navegadores también tienen programas de mensajería al igual que la mayoría de sitios de redes sociales como Facebook y MySpace.

Muchos programas de mensajería instantánea tienen "localizadores de amigos en línea" lo que significa que a usted le avisan cuando uno de sus amigos ha entrado en línea. Los depredadores pueden tener muchos localizadores

de amigos en línea. Todo lo que tienen que hacer es sentarse y esperar a que cierto niño entre en línea.

Muchos programas de mensajería instantánea también pueden transferir archivos incluyendo archivos de fotografías, sonido y video. A través de los programas de mensajería instantánea también se puede utilizar el video y la voz. Los depredadores usualmente utilizan las pláticas de texto para esconder su edad y parecer ser otro niño.

Los programas de mensajería instantánea también le permiten tener múltiples conversaciones de manera simultánea. Los depredadores con frecuencia hacen esto para eliminar los niños poco receptivos y encontrar a un niño que pueda ser preparado con atención y simpatía para una relación sexual.

Teléfonos celulares y mensajes de texto

A los chicos les encanta usar los teléfonos celulares para enviar y recibir mensajes de texto. Los teléfonos celulares también pueden enviar y recibir fotos, video y otro tipo de archivos.

Una vez que el depredador establece contacto con un niño, puede usar mensajes de texto para comunicarse. El niño puede estar en la escuela, con sus amigos o en cualquier otro lugar lejos de sus padres. El depredador también puede llamar y hablar al niño. Enseñe a los niños a nunca dar su número de teléfono celular a nadie que no conozcan en el mundo real.

La comunicación en línea tiene su propio lenguaje abreviado. Este se usa en correos electrónicos y mensajes de texto para ahorrar tiempo y pulsaciones de teclas. También evita que los “intrusos” entiendan lo que dicen los mensajes.

Sexting (mensajes de texto sexuales)

"*Sexting*" es la práctica de enviar fotos suyas desnudo o parcialmente desnudo a través del teléfono celular. Es muy popular entre los niños. Ocurre todos los días en Idaho, todos los días en nuestras escuelas. Por lo general son chicas que toman fotos de sí mismas con su teléfono celular y las envían a alguien más, con frecuencia su novio.

En el año 2008, un estudio para la Campaña nacional de prevención de embarazos adolescentes y no deseados, encontró que el 22% de las chicas adolescentes y el 18% de los chicos adolescentes había enviado o publicado fotos de sí mismos desnudos o parcialmente desnudos. El 11% de las chicas adolescentes (13 – 16 años de edad) admitieron haber hecho esto.

Parte del problema es que una vez usted envía la foto a través del teléfono celular, perdió el control de esta. La persona a la que se la envía se la puede enviar a otras personas. Estas fotos con frecuencia terminan en la Internet y causan problemas años más tarde cuando llegue el momento de conseguir un trabajo o ingresar a la Universidad. Algunos chicos han perdido becas cuando una universidad realizó una revisión de los antecedentes y encontró este tipo de fotos en línea.

En algunos casos, el *sexting* puede ser un delito con agravante calificado. Enviar fotos de desnudos o guardar fotos de desnudos de cualquier persona menor de 18 años puede ser procesado como pornografía infantil. Un niño que hace esto puede ir a prisión. Algunos chicos han sido procesados por enviar o poseer fotos que pensaron que era un chiste.

Consejos para los adolescentes

- Piense en las consecuencias de tomar, enviar o reenviar una foto sexual de alguien menor de edad, inclusive si es suya. Usted podría ser sacado de equipos deportivos, enfrentar la humillación, perder oportunidades educativas, y hasta tener problemas con la ley.
- Nunca tome fotos suyas que no desearía ver en la cartelera de la escuela o en el refrigerador de su familia.
- Antes de presionar la tecla enviar, recuerde que usted no puede controlar a dónde llegará esa foto. Lo que usted le envía a un novio o novia podría fácilmente terminar en manos de sus amigos.
- Si reenvía una foto sexual de alguien menor de edad, usted es responsable de esta imagen como lo es el remitente original. Usted podría enfrentar cargos por pornografía infantil, ir a prisión y tener un registro como delincuente sexual.
- Informe acerca de cualquier foto desnuda que reciba a su teléfono celular o computadora a un adulto en el que confíe. No borre el mensaje. En vez de esto, apague su teléfono celular y haga que sus padres, profesores y consejeros de la escuela u oficiales que hacen aplicar la ley se involucren inmediatamente.

Consejos para padres

- Hable con sus hijos. Establezca reglas para el uso del teléfono celular.
- Si sus hijos no necesitan tener el servicio de mensajes de texto, cancélelo.
- Limite el tiempo que sus hijos pasan hablando por

teléfono celular. Si no necesitan un teléfono celular, no se los de.

- Ha habido muchos casos en los que los niños están despiertos toda la noche enviando mensajes de texto desde su teléfono. Este es un buen momento de colocar el teléfono en el cargador.

SITIOS DE REDES SOCIALES

Visión general

En los sitios de redes sociales, la gente crea páginas personales llamadas "perfiles" para comunicarse con otras personas en línea. Facebook, MySpace, MocoSpace y YouTube son los sitios más populares entre los adolescentes.

Cualquier persona con acceso a Internet puede crear un perfil en un sitio de redes sociales. Una vez que la persona crea un perfil, esa persona (o "miembro") puede publicar información personal, fotos y "blogs" en el perfil para que otras personas lean. Los miembros enlazan sus perfiles a través de redes de "amigos", ven los perfiles de los demás, comparten fotos y publican comentarios. Desafortunadamente, los depredadores sexuales usan los sitios de redes sociales para conocer y preparar víctimas en línea.

JUEGOS EN LÍNEA Y MUNDOS VIRTUALES

Sistemas de juego en línea

La mayoría de los sistemas de video juego más recientes (por ejemplo Wii, PS3, Xbox, etc.) tienen la opción de conectarse a Internet para juegos interactivos. Estos nuevos sistemas de video juegos permiten a los jugadores de cualquier parte del mundo conectarse y competir contra otros usando muchos juegos populares. Una vez conectados, pueden comunicarse

usando salas de plática de juego. Varios sistemas también tienen la capacidad de añadir cámaras web y audífonos, lo que les permite a los jugadores hablar y ver a los demás jugadores. Esto es parte de la experiencia de juego "interactiva, en vivo". Desafortunadamente, esta tecnología brinda a los depredadores una oportunidad de ver y hablar con su hijo. Un depredador podría tratar de hacer que el niño se desvista, o escoger a un niño que encuentre atractivo para un secuestro.

Los sistemas de juego en línea tienen muchos controles para padres que permiten a los padres establecer opciones para el juego en línea de sus hijos. Usted puede enterarse mejor al leer el manual del usuario que viene con el sistema de juego, revisar los menús del sistema de juego o visitar el sitio Internet del fabricante del sistema de juegos.

Sitios de juegos en Internet

Algunos sitios de juegos en Internet ofrecen juegos "con pláticas supervisadas". Esto puede proporcionar un falso sentido de seguridad. No confíe en eso. ¿Sabe usted quienes son los supervisores? ¿Desea permitirles que cuiden la seguridad de su hijo? Una plática supervisada puede rápidamente conducir a una plática no supervisada, por ejemplo un intercambio de direcciones de correo electrónico.

Consejos para jugar en línea de manera segura

- Vea las clasificaciones de juego y preseleccione los juegos en línea antes de comprarlos.
- Revise para ver si la consola viene con las características de control para padres.
- Establezca los controles para padres antes de que los niños comiencen a jugar.
- Coloque las consolas de juego en un área común de

la casa donde los adultos puedan controlar la actividad.

- Decida si desea usar las capacidades de la consola para Internet.
- Establezca las reglas de juego con sus hijos, como por cuánto tiempo y con quién pueden jugar.
- Ayude a sus hijos a seleccionar nombres de pantalla adecuados para su edad y que no demuestren su género.
- Decida si desea permitir la plática de voz. Si no, utilice las características de protección de voz.
- Enseñe a sus hijos a no reveler información personal a través de la plática de voz.
- Anímelos a que no respondan a ciberacoso y a que bloqueen cualquier contacto no deseado.

Mundos virtuales

Los mundos virtuales están creciendo en popularidad en la Internet. *Second Life* es uno de los más populares.

En un mundo virtual, usted puede crearse a sí mismo, una representación de sí mismo llamado un avatar. Su avatar puede ser quien usted desee que sea o hacer lo que usted desee que haga. Inclusive puede crear un avatar que vuela.

Second Life tiene su propio dinero, llamado *Linden dollar*. Para tener una segunda vida satisfactoria, usted necesita dinero para comprar una propiedad, construir una casa, comprar cosas y participar en actividades.

En *Second Life* usted puede hacer cosas para obtener dinero o puede comprar dinero *Second Life* en el mundo real, por ejemplo, en realidad puede comprar *Linden Dollars* en

EBay. Ese dinero tiene correlación directa con el dólar estadounidense.

En *Second Life* usted puede comprar algo llamado "*Capture Scent*." Si su avatar se encuentra con el "*Capture Scent*" de otro avatar, esto dejará a su avatar inconsciente durante diez minutos y el otro avatar puede hacer lo que quiera con su avatar.

También tiene escenas sexuales, con los avatars participando en actividad sexual.

Las personas pueden incorporar videos o fotos en cualquier parte de *Second Life*. Por lo tanto si un niño está visitando la casa de alguien en *Second Life*, podría estar viendo pornografía.

Los mundos virtuales como Second Life no son lugares para niños.

CIBERACOSO

El ciberacoso ocurre cuando los niños utilizan la Internet, teléfonos celulares u otros aparatos digitales para enviar o publicar mensajes o imágenes con la intención de herir, humillar o avergonzar a otra persona. Muchos adolescentes se ven agobiados cuando alguien roba su contraseña u otra información personal y envía mensajes perjudiciales desde su correo, sitio personal o página de red social. La capacidad de la Internet de llegar a grandes audiencias en segundos la hace el lugar perfecto para amigos, enemigos y los anónimos para acosar a otros adolescentes.

Ningún niño debería aguantar el ciberacoso u hostigamiento. Enseñe a sus hijos a contarle a usted inmediatamente si otros niños están diciendo cosas malas sobre ellos o haciendo amenazas.

Formas de ciberacoso

Existen muchos tipos diferentes de ciberacoso. A continuación aparecen tan solo unos cuantos ejemplos:

- Enviar o reenviar mensajes de texto, correos electrónicos o conversaciones malas, amenazadoras, discriminadoras, humillantes y embarazosas; o vengativas;
- Burlarse o asustar a alguien en línea;
- Usar comentarios o lenguaje lascivo o insultante;
- Usar la contraseña de alguien más para acceder a la cuenta de esa persona;
- Hacerse pasar por alguien en línea;
- Difundir rumores o mentiras sobre alguien a través de mensajes, comentarios, anuncios o publicaciones en muros;
- Fingir ser alguien que usted no es para reunir información de otras personas;
- Publicar fotos o información sobre alguien sin su consentimiento;
- Insultar a alguien mientras se juega un juego interactivo en línea;
- Votar en un sondeo o libro de visitas de críticas.

Poner fin al ciberacoso

Hable con sus hijos sobre el ciberacoso y cómo este podría afectarlos, tanto como víctima o como participante. Asegúrese que sus adolescentes entiendan que deben tratar a los demás con respeto cuando están enviando mensajes de texto o cuando están en línea, y que existen fuertes consecuencias legales para el ciberacoso en Idaho.

La mayoría del ciberacoso comienza en pequeño, pareciendo privado, entre amigos y luego crece rápidamente en un foro público hasta llegar a estar fuera del control del instigador. Todas las personas son un blanco potencial. La mitad de los estudiantes admiten haber sido acosados en línea, mientras que un estimado del 79% de los adolescentes dicen que es un problema.

Lo más importante que usted puede hacer es permitir que sus adolescentes sepan que pueden acercarse a usted si sienten que están siendo víctima del ciberacoso.

Usted puede ayudar a sus adolescentes a permanecer seguros al hacer que sigan estos pasos:

- No reenviar ni responder nunca a mensajes o imágenes malas, embarazosas o hirientes (los chicos llaman a estos mensajes "llamas"). Los acosadores con frecuencia acosan a otras personas para provocar una reacción que luego alimenta un mayor acoso.
- Bloquear cualquiera y todas las comunicaciones de un ciberacoso. Los programas spyware han sido creados para enviar mensajes de acoso anticipando la respuesta del blanco.
- Borrar a los "amigos" o "cuates" si publican comentarios o imágenes que son malas, embarazosas, amenazantes o acosadoras.
- Nunca compartir contraseñas u otra información de cuenta con nadie.
- Nunca entregar su información personal a nadie.
- En los sitios de redes sociales, seleccionar la opción que permite prever todos los comentarios y publicaciones de otro usuario antes de que sean públicos.

- Reportar cualquier acoso. Contar a un adulto confiable y reportarlo a su proveedor de servicio de Internet o sitio Internet (por ejemplo, Facebook, MySpace, etc.). Llamar a la policía si lo amenazan. Reportar el ciberacoso en línea en www.cybertipline.com y ante el policía asignado a la escuela.

Existen leyes en Idaho que protegen a las víctimas de hostigamiento, intimidación y acoso. Si usted considera que su hijo es víctima de ciberacoso, hable de inmediato con el consejero de la escuela o el policía asignado a la escuela. El ciberacoso puede tener efectos muy serios sobre su hijo.

APÉNDICE A

Recursos en línea

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

www.ag.idaho.gov

ProtecTeens, un video educativo y paquete de recursos para manejar la seguridad infantil en línea está disponible en el sitio Internet del Fiscal General. Esta Publicación y otras publicaciones de protección al consumidor también están disponibles.

www.icacidaho.org

El sitio de la *Idaho Internet Crimes Against Children Task Force* (Fuerza especial de crímenes en Internet contra niños de Idaho) ofrece consejos que los padres pueden usar para proteger a sus hijos de la explotación criminal en línea.

www.ic3.gov

El *Internet Crime Complaint Center* (IC3) (centro de denuncias de delitos en Internet) recibe denuncias relacionadas con delitos en Internet y los remite a las agencies de aplicación de la ley y reguladoras a nivel federal, estatal, local e internacional.

www.fraud.org

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

www.netsmartz.org

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

www.consumer.gov

Este sitio Internet de la agencia federal proporciona publicaciones e información para el consumidor.

www.pueblo.gsa.gov

El *Consumer's Resource Handbook*, (manual de recursos del consumidor) disponible en este sitio 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 *Federal Trade Commission* (comisión federal de mercadeo) ofrece folletos en línea relacionados con las compras en Internet y estafas de correo electrónico o 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 archive 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 ubicados en el disco duro de su computadora, de algunos sitios de Internet que usted visita.

Download **(descargar)** – Copiar archivos de 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 División 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 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 archive 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.

Manuales de protección al consumidor

Donaciones a instituciones benéficas
Foreclosure Prevention: A Workbook *
Guidelines for Motor Vehicle Advertising in Idaho *
Manual de protección al consumidor de Idaho
Ley del limón de Idaho
Seguridad en Internet
Guía del dueño y el inquilino
Construcción residencial
Manual para adultos mayores de 60 años
Service on an Idaho Nonprofit Board of Directors *
Solicitaciones Telefónicas
Manual del joven adulto

*Sólo en inglés

Esta publicación fue preparada por la División de Protección al Consumidor de la Oficina del Fiscal General y la Idaho Internet Crimes Against Children Task Force (Idaho ICAC) (Fuerza especial de crímenes en Internet contra niños de Idaho).

Los fondos para pagar esta publicación provinieron de subvenciones que obtuvo la División de Protección al Consumidor de la Oficina del Fiscal General. No se utilizó dinero proveniente de impuestos para pagar este folleto.

La División de Protección al Consumidor hace cumplir las leyes de protección al consumidor de Idaho, brinda información al público acerca de los asuntos del consumidor y ofrece un proceso de mediación informal para quejas particulares de los consumidores.
Si tiene un problema o una pregunta como consumidor, por favor, llame al (208) 334-2424 ó gratis en Idaho al (800) 432-3545. Están disponibles el acceso TDD y los servicios de interpretación Language Line. La página de Internet del Fiscal general está disponible en www.ag.idaho.gov.

Si tiene información respecto a un crimen por Internet en contra de un niño o si piensa que una información sería útil en la lucha contra la explotación infantil, contáctenos a través de la línea nacional CyberTipline en www.cybertipline.com o llame gratis al (800) 843 5678. La información que usted proporcione se enviará a las agencias correspondientes de cumplimiento de la ley ICAC en Idaho o en cualquier otro lugar de los Estados Unidos.

Última revisión 6/2015