Políticas de Seguridad

Seguridad en Internet

La presente información tiene por objeto recomendar y sugerir las mejores prácticas a seguir por cada usuario de la página de ILC. Todos los términos y condiciones incluidos en la página de ILC resultan aplicables.

- Para ILC es necesario y de suma importancia mantener la información de sus clientes en forma segura y confidencial. ILC continúa esforzándose por mantener el más alto nivel de seguridad para sus clientes, su información y sus transacciones.
- Los usuarios de la PAGINA ILC representan un rol crítico en la función de mantener protegida su información personal. Por lo tanto, le recomendamos revisar cada sección de la PAGINA ILC y familiarizarse con las medidas que ILC tiene en cuenta en la protección de su información, así como respecto de las sugerencias a seguir a fin de asegurar su experiencia en línea a través de la PÁGINA ILC.

Uso fraudulento del correo electrónico

Medidas preventivas

- Evite abrir correos electrónicos o archivos adjuntos enviados desde fuentes desconocidas, ya que podrían incluir algún virus (mayor detalle en la sección "Glosario de Términos") y dañar su computadora. Realice una revisión con su software antivirus previamente.
- Evite responder correos electrónicos que soliciten información personal.
- Únicamente realice operaciones con compañías en las que confíe. Si tiene dudas, siempre contacte a la compañía por teléfono y consulte por la solicitud de información personal enviada por correo electrónico.

Correo Electrónico Phishing

Es aquel que se hace pasar por un correo electrónico legítimo de una organización, adjuntando enlaces o links a páginas falsas donde se solicita información confidencial que puede ser utilizada para cometer algún tipo de fraude. Si usted recibe un correo electrónico o un link solicitando la confirmación de información personal, no ingrese la información.

Correo electrónico del tipo "Spam"

Es usual que algunas compañías adquieran listas de correos electrónicos, para enviar publicidad por este medio. Estos correos no solicitados se denominan "Spam", y llenan rápidamente los buzones de correo, además de lanzar ventanas automáticamente ("pop-ups") al abrirlos. Usted puede adquirir software anti-spam para filtrar correos electrónicos no deseados o "spam".

Correo electrónico del tipo "Cadena"

Un correo electrónico que solicita a quien lo recibe, que lo reenvíe a todos los que conoce, se denomina "Cadena". Muchas compañías que venden listas de correos también envían correos cadena, y cada persona que responde o es adicionada en la lista de direcciones, se une a la lista de la cadena. Las personas responden a las cadenas debido a que en ellas se promete obtener dinero o buena suerte. Lo mejor es eliminar los correos electrónicos cadena debido a que los archivos adjuntos pueden contener algún virus informático. También es posible instalar programas anti-spam para bloquear correos no deseados.

Virus informáticos e infecciones

Protéjase asimismo contra virus (mayor detalle en la sección "Glosario de Términos") y correo electrónico fraudulento. Su mejor defensa contra virus por computadoras es disciplina y educación, ambos ayudan a reducir el riesgo de ser víctima de virus informáticos. Además de lo antes indicado, le recomendamos lo siguiente:

- Instale programas anti-spam para reducir el número de correos electrónicos potencialmente peligrosos.
- Ejecute un programa antivirus actualizado de manera frecuente en su computadora. El software antivirus puede escanear los correos de entrada y salida, así como los archivos adjuntos, en busca de gusanos, virus informáticos, Caballos de Troya, entre otros.
- Nunca dé doble click en un archivo adjunto que sea un programa ejecutable, que contenga la extensión "exe", "com", o "vbs", a menos que pueda confiar en la fuente. En caso un archivo sea infectado con un virus (mayor detalle en la sección "Glosario de Términos") y se abra, el virus puede dañar el disco duro, archivos de programa, y archivos de correo electrónico. Ejecutando un software antivirus usualmente se detectan infecciones antes de que cualquier archivo sea abierto.
- Lea la política de privacidad de las páginas Web que visite. Las políticas de privacidad han sido diseñadas para informar a los clientes sobre los detalles de cómo su información personal se mantiene de manera confidencial, como se comparte y por qué se necesita. Es una buena práctica leer las políticas de privacidad de toda compañía con la que realice transacciones

financieras. Muchas políticas de privacidad explican cómo se puede solicitar remover su nombre de las listas de dirección de correo electrónico.

Recomendaciones

La seguridad de su información es prioridad para ILC. Nuestros sistemas y procedimientos de seguridad han sido diseñados para mantener su información personal de manera confidencial en todo momento. Usted tiene un importante rol que cumplir en cuanto a la seguridad de su información y debe adoptar las siguientes prácticas para ayudar a mantener su información protegida contra usos no autorizados:

Le recomendamos tomar acción para prevenir que su información sea obtenida por terceros en forma no autorizada, siguiendo los siguientes pasos:

Recomendación para usuarios de Microsoft Internet Explorer.

Por defecto, Microsoft Internet Explorer utiliza el disco duro de la computadora para mantener una copia de todas las páginas, imágenes y archivos recientemente visualizados. A pesar de visualizar una página protegida con SSL (Secure Socket Layer, ver la sección "Glosario de Términos"), gran parte de la información más sensible se mantiene en el disco duro de su computadora luego de cerrar el navegador Web.

Recomendaciones para usuarios de Netscape Navigator

Si usted se encuentra utilizando una versión actualizada de Netscape Navigator (7.2 o más), no almacenará información en su disco duro cuando navegue por una página protegida con SSL (Secure Socket Layer, ver la sección "Glosario de Términos"). En ese sentido, los usuarios de Netscape no requieren realizar configuraciones adicionales. En caso esté utilizando una versión anterior de Netscape Navigator, se recomienda efectuar la actualización a la más reciente.

Recomendaciones para adoptar las mejores prácticas "Online"

Nunca ingrese información personal en formularios o aplicaciones de Internet en los que no se muestre, antes de la dirección Web lo siguiente: "https://...", o el símbolo de un candado en la esquina inferior derecha del navegador Web. Comúnmente, estos símbolos indican que la página funciona con información encriptada, y la información ingresada está protegida.

Recomendaciones para proteger su computadora personal

- Instale un Firewall personal (mayor detalle en la sección "Glosario de Términos") en sus computadoras personales, para prevenir acceso no autorizado que pueda poner en riesgo sus archivos, permitir acceso a información personal o la destrucción de la misma. Esto es especialmente importante en computadoras que utilizan conexiones dedicadas a Internet. Debido a que la conexión con Internet se habilita al encender la computadora, el riesgo de sufrir ataques en su computadora aumenta.
- Ejecute un programa antivirus en su computadora personal de manera frecuente para prevenir que algún virus informático o gusano (mayor detalle en la sección "Glosario de Términos") ingrese en el sistema. Asimismo, adquiera programas que automáticamente actualicen su protección antivirus de manera regular.
- No permita el acceso a su computadora por parte de terceros y extraños.
- Deshabilite la capacidad de compartir archivos e impresoras en su computadora personal para prevenir que algún tercero desde Internet navegue o elimine sus archivos.
- Revise la documentación propia de su computadora personal para realizar las configuraciones o acceda a la página Web de su proveedor.
- De manera regular, revise la página Web del sistema operativo de su computadora personal (por ejemplo Microsoft Windows) para descargar parches o actualizaciones al sistema o al navegador, y asegurar que su computadora personal cuente con las últimas actualizaciones de seguridad instaladas.
- Infórmese sobre ataques de algún virus informático y esté al tanto de los últimos gusanos, virus, caballos de Troya (mayor detalle en la sección "Glosario de Términos") u otros programas maliciosos diseñados para dañar su computadora personal y/o apropiarse de información de la misma.
- Evite abrir correos electrónicos o archivos adjuntos recibidos de fuentes desconocidas y en todo caso, utilice su programa antivirus para revisar los correos previamente.

¿Cómo Protegerse?

Protéjase a sí mismo "Online"

Tenga cuidado especial y verifique la fuente de algunas páginas Web que han sido diseñadas para confundir a los consumidores y recolectar información personal. Lea las políticas de privacidad de las páginas Web que visite para aprender cómo manejan la privacidad de su información personal y cómo dirigen ofertas por correo electrónico, publicidad, promociones, entre otros.

- Nunca brinde información personal a ningún tercero por teléfono o a través de una página Web, a menos que haya verificado la credibilidad de la fuente. Las compañías de buena reputación, nunca le solicitarán su contraseña o número de identificación personal (PIN) por correo electrónico o por teléfono.
- Firme sus tarjetas de crédito y de débito al momento de recibirlas. Una tarjeta no firmada puede ser fácilmente suscrita en caso de pérdida, robo o sustracción. Reporte las pérdidas o robos de tarjetas de crédito o de débito de manera inmediata a la entidad financiera respectiva. Revise sus transacciones luego de la pérdida, robo o sustracción y notifique a la entidad financiera en forma inmediata en caso de haber detectado o sospeche de alguna transacción efectuada sin su autorización.
- Notifique a su institución financiera si desea cancelar una tarjeta de crédito o de débito e inmediatamente destruya la tarjeta cancelada cortándola y atravesando el número de cuenta y la banda magnética.
- Espere por sus recibos de consumo y de cajero automático, y no los deje en bolsas de compras ni en las tiendas. Tenga cuidado con la información personal que pueda desechar. Asegúrese de destruir todos los recibos, rastros de movimientos bancarios y cuentas que puedan contener información personal. Destruya las copias de carbón, y una vez que verifique sus transacciones, destruya los recibos en casa.
- Al utilizar cajeros automáticos, ubíquese de tal manera que nadie pueda visualizar el PIN. Atienda a su alrededor y si sospecha de alguna actividad ilegal en un cajero automático, retírese inmediatamente y contacte a la policía y a la entidad financiera.
- Mantenga sus cheques, chequeras, movimientos de cuenta, y demás documentos relacionados a sus transacciones financieras en un lugar seguro. No deje sus pertenencias, carteras, chequeras o tarjetas de crédito o de débito fuera de su atención.

Glosario de Términos

Programas Anti-virus

Su computadora personal o Laptop debe contar necesariamente con programas antivirus instalados para prevenir infecciones por parte de virus a través de correos electrónicos y archivos de programas. Adquiera un programa que automáticamente actualice la versión de su antivirus de manera regular.

Navegadores Web

Un navegador Web es una aplicación que trabaja con Internet para proveer la capacidad de visualizar, encontrar e interactuar con páginas Web.

Cable Módem

Cable Módem provee acceso a Internet a una alta velocidad, utilizando redes de televisión por cable. Cable Módem ofrecen conexión continua a Internet sin la necesidad de establecer conexión con un proveedor de servicios de Internet (ISP) al iniciar la conexión con Internet.

Cookies

Las "cookies" son pedazos de información almacenada en la computadora. Contienen información referente a las preferencias de la configuración en su computadora que permiten que las páginas Web a las que accede, se ajusten a sus preferencias. Cada vez que ILC utiliza una "cookie", la información personal es encriptada para nuestro uso únicamente, y protegida del acceso a terceros.

Certificados Digitales

Los Certificados Digitales ayudan a individuos y organizaciones en Internet a poder identificarse entre sí y prevenir accesos no autorizados. El navegador mantiene esta información y la utiliza para certificar la autenticidad de la información enviada hacia usted.

Encriptación

Cuando puede visualizar https:// al inicio de la dirección Web en la barra de direcciones del navegador, o cuando aparece un candado en la esquina inferior izquierda de su navegador, significa que su sesión es segura, ya que se encuentra encriptada.

Firewall

Un Firewall puede ser instalado ya sea en una computadora de su casa o de su negocio, como medida de protección ante hackers y virus informáticos. Los "Firewalls" son utilizados para filtrar información dañina para su computadora y para prevenir accesos no autorizados a ella.

Captura de tecleo

Existen herramientas que almacenan en memoria todas las teclas que son presionadas en un teclado, con el objetivo de obtener contraseñas e información de inicio de sesión.

Plug-in
Un "plug-in" es un módulo de programa que adiciona una funcionalidad específica en el navegador Web. Por ejemplo, los "plug-ins" para Internet Explorer o Netscape Navigator, permiten que los navegadores muestren distintos tipos de sonidos y video.
Huecos de seguridad y bugs (Debilidades de seguridad)
Son defectos o errores de programación explotados por determinados usuarios no autorizados para ganar acceso a redes de computadoras o servidores en Internet. A medida que estas debilidades se hacen conocidas, los fabricantes publican "parches" o "actualizaciones" que los usuarios pueden descargar para solucionar los problemas.
Ingeniería social
Ingeniería social es un proceso por el cual se sustrae información por medio de la interacción humana, y casi siempre involucra el engaño a un individuo para que éste le provea información personal, como detalles de cuentas de clientes o contraseñas. La información personal se utiliza luego para aplicar a créditos, compras, o acceder a cuentas bancarias.
Spam
Algunas veces las compañías o individuos pueden adquirir listas de correos electrónicos para enviar avisos de venta de productos y servicios. Estos correos no solicitados se denominan "Spam" y llenan las casillas de correo de los usuarios. Usted puede adquirir programas anti-spam para filtrar correos no solicitados o spam de su lista de correos.
Phishing
Una manera de sustracción de propiedad privada que se está utilizando cada vez más, es el "phishing". El "phishing" involucra que un correo electrónico sea enviado a todas las direcciones de correo que se puedan obtener, haciéndose pasar por una organización legítima como un banco, compañía de pago de servicios en línea o similar. El correo solicita actualizar información personal del usuario como nombre de usuario, fecha de nacimiento, números de tarjetas de crédito, entre otros. El objetivo es hacer creer a las víctimas que el atacante es un miembro legítimo de la organización de la cual dice pertenecer, para que respondan y envíen la información al atacante.
El correo contendrá un link que le llevará a una página Web que luce idéntica o al menos bastante similar a la original. Para evitar este tipo de delitos, nunca responda a correos electrónicos que soliciten información personal o financiera, y nunca acceda a links de estos correos.
Caballo de Troya
Un Caballo de Troya es otro tipo de virus informático, representado en un programa de computadora que se hace pasar por otro programa. Para disminuir el riesgo de infección, es importante ejecutar los programas antivirus previamente a abrir los programas.
Virus
Un virus informático es un pequeño programa que se introduce por si sólo en correos electrónicos y archivos de programas. Algunos virus se propagan a través del correo electrónico y luego se replican reenviándose automáticamente a toda la lista de contactos del correo afectado.
Gusano
Un virus del tipo Gusano es un pequeño programa que busca en diferentes redes de manera aleatoria para encontrar "agujeros de seguridad" (debilidades de sistema) con el objeto de replicarse a sí mismo de computadora a computadora.
SSL
Significa "Secure Socket Layer" y ayuda a verificar que la información sensible (números de tarjetas de crédito, e información financiera en general) enviada por Internet entre su navegador y un servidor Web, se mantiene de manera confidencial durante las transacciones en línea.

****