unidad 11

seguridad informática

contenidos

- Propiedad intelectual y legislación
- Seguridad y privacidad de la información

Acerca de esta unidad

La seguridad informática es una especialización dentro de la informática que busca implementar las técnicas y tecnologías adecuadas para evitar que la privacidad e integridad de la información se vean afectadas por actos delictivos.

Para poder cumplir con sus objetivos, la seguridad informática se apoya en herramientas de hardware, software, recursos humanos especializados en técnicas especiales de seguridad y la legislación vigente en cada país.

En esta unidad trataremos temas como: propiedad intelectual y legislación, derechos de autor, licencias, software libre y software propietario, protección de la información y virus informáticos.

Vocabulario: busca en el diccionario las siguientes palabras

Derecho	Legislación	Restringir
Estímulo	Licencia	Retribución
Jurídico	Masivo	Vulnerar

Los términos técnicos se encuentran en el glosario.

Propiedad intelectual y legislación

Derechos de autor

La **propiedad intelectual** consta de los derechos que un autor tiene sobre su obra y, como en cualquier otro rubro, en la informática también se debe respetar.

Gracias a las facilidades que brinda la Web para copiar y reproducir información digital, los usuarios pueden intercambiar archivos casi sin ningún tipo de restricción; pero hay que ser cuidadosos en torno a la utilidad que se le da a esos archivos –sea una canción, un programa o una imagen–, teniendo siempre en cuenta si tiene derechos reservados y qué tipo de licencia habilita el uso –y bajo qué condiciones– del recurso en cuestión.

El creador de una obra espera que se respeten sus derechos de autor, de lo contrario el estímulo, que hasta ahora ha sido importantísimo para la creación intelectual, se verá afectado.

Publicar en Internet no es sinónimo de autores que renuncian a una retribución por su trabajo, ni que las organizaciones produzcan y distribuyan información gratuitamente.

Afortunadamente para todos, cada vez cobran más auge las herramientas de software libre que poco a poco van afianzándose como alternativas reales a los productos comerciales.

¡Atención!

Que en Internet, debido a su estructura, descentralización y calidad de entorno democrático, sea más fácil vulnerar los derechos de autor no quiere decir que tenga sentido hacerlo.
Todavía se necesita un intenso trabajo sobre nuevos instrumentos jurídicos y tecnológicos para asegurar la protección del material propietario, sin restringir el acceso al usuario.

Licencias

Una **licencia de software** (Software License) es la autorización o permiso concedido por el titular del derecho de autor, en cualquier forma contractual, al usuario de un programa informático, para utilizar éste en una forma determinada y de conformidad con condiciones convenidas.

La licencia puede ser gratuita o comercial y detalla los derechos del usuario o comprador en cuanto a:

- Uso. Explica qué tipo de utilización puede darle el usuario al software.
- Modificación. Se establece si está permitido o no que el usuario modifique el producto.
- Distribución. Establece bajo qué condiciones se puede copiar o no el programa.
- Plazo de duración de la licencia.
- Los límites geográficos en donde se aplica.

GPL

Los tipos de licencia que existen son muchos y variados, pero en temas anteriores hemos mencionado en varias oportunidades la licencia GPL.

La licencia **G**eneral **P**ublic **L**icense (GPL) es la licencia que se aplica a los programas o documentos que son software libre, y tiene como objetivo primordial asegurar que el software que es libre siga siéndolo a través del tiempo y más allá del uso que cada usuario realice.

Software libre vs. Software propietario

Es importante entender los conceptos de software libre y software propietario o software no libre para poder utilizar los recursos que estos programas brindan con el debido conocimiento del marco legal que los regula.

El **software libre** permite que un programa sea copiado, distribuido, investigado, modificado, etc. sin ningún tipo de restricción y, en general, se lo encuentra como software gratuito publicado en Internet.

Sin embargo, al ser software libre, un usuario o empresa puede tomar un programa libre, modificarlo de acuerdo a sus necesidades y venderlo como producto comercial propio. La empresa no puede evitar que el software original que utilizó y dio origen a su nuevo producto, deje de ser software libre. La licencia GPL se encarga de hacer perdurar el estatus de libre a todo software que lo sea.

En cambio el **software propietario** es todo programa que tiene limitaciones para ser copiado, implementado y distribuido. El código fuente no se encuentra disponible al público en general, siendo los únicos autorizados a acceder a él los propietarios del programa, quienes tienen los derechos exclusivos sobre el producto y la tecnología.

Tanto el software libre como el propietario siempre deben ir acompañados por la correspondiente licencia que defina las responsabilidades y obligaciones del usuario y los autores.

Tipo de versiones de software

El usuario puede obtener distintas versiones de cada producto de software. Cuando se descargan programas de la Web es necesario tener en cuenta el tipo de licencia y versión del producto para no incurrir en una violación a la propiedad intelectual en perjuicio del autor.

El autor o los autores de un producto informático pueden brindar versiones de prueba, o con limitaciones, para que los usuarios evalúen las capacidades de dicho producto.

Cuando el software es **free software** significa que es de libre uso y que el usuario puede instalar y utilizar la herramienta informática sin ningún tipo de retribución obligatoria al autor –de todas formas siempre hay que leer atentamente la licencia que acompaña al programa–. El freeware es similar pero puede o no incluir el código fuente de la herramienta.

La característica de **shareware** indica que el programa se puede instalar en la computadora pero que no cuenta con toda la funcionalidad que tiene la versión comercial –tiene opciones deshabilitadas, no permite grabar las modificaciones en los datos, no permite imprimir o limitaciones similares–. Es una versión que permite usar el programa todo el tiempo que se desee, pero con las limitaciones mencionadas, y para obtener toda la funcionalidad se debe pagar el precio de la versión comercial.

La versión **demo** o **trial** es similar a la shareware, con la diferencia que tiene un período de uso –estipulado por ejemplo en días o meses– y puede o no estar limitado en las funciones que realiza.

En cambio, si el programa está en versión **beta** significa que es una versión que todavía puede contener errores –está en etapa de desarrollo– y que se pone a disposición de los usuarios para que opinen sobre posibles cambios a realizar antes de la aparición de la versión comercial. Las versiones beta, por ser versiones en desarrollo, son gratuitas.

Seguridad y privacidad de la información

Protegiendo la información

La **seguridad informática** es una especialización dentro de la informática que busca implementar las técnicas y tecnologías adecuadas para evitar que la privacidad e integridad de la información se vean afectadas por actos delictivos llevados a cabo por "piratas informáticos".
Para poder cumplir con sus objetivos, la seguridad informática se apoya en herramientas de hardware, software, recursos humanos especializados en técnicas especiales de seguridad y la legislación vigente en cada país.

Consejos para cuando te conectas a Internet

Al conectarnos a Internet nos exponemos a ciertos riesgos relacionados con la privacidad de las personas y la mala utilización de nuestra información personal. Aquí, algunas pautas a tener en cuenta para que la experiencia sea lo más segura y positiva posible:

- Al dejar de usar la PC siempre se debe **cerrar la sesión de las cuentas y de los mensajeros** que se estén utilizando; de esta forma se evita que personas, sin autorización, accedan a las cuentas.

- En un locutorio o cíber café se debe **tener especial cuidado con las claves**. Si se debe hacer transacciones comerciales o financieras a través de Internet que impliquen escribir con el teclado números de cuentas bancarias o de tarjetas de crédito, usar siempre el teclado virtual, de estar presente en el sitio Web que soporta la transacción. Existen programas que capturan las pulsaciones del teclado y esto permite averiguar datos muy importantes, con las consecuencias que esto implica.

- Al acceder a Internet desde un locutorio o cíber café se aconseja **no hacer clic** en las opciones que suelen aparecer en mensajeros y/o webmail: Recordar clave. Al activar esta opción la PC recuerda el nombre de usuario y contraseña, permitiendo que cualquier persona ingrese a la cuenta de la persona que usó la PC anteriormente. Así que, cuando la PC es de uso público, no es recomendable activar esta opción.

- En Internet, **nunca se deben brindar datos personales de ningún tipo**. Si bien al abrir una cuenta de correo hay que ingresar algunos datos, es optativo que sean reales o no; además en este tipo de proceso nunca se solicitan números de teléfono, de tarjetas de crédito o de cuentas bancarias.

Importante

Los términos hacker y cracker hacen referencia a personas con un gran conocimiento en dispositivos de hardware y herramientas de software.

Lo que diferencia a estos expertos es su forma de proceder, mientras que el hacker utiliza sus conocimientos para probar la vulnerabilidad de los sistemas de una forma solo intrusiva, los cracker acceden a los sistemas informáticos con intenciones destructivas o delictivas.

Privacidad de la información

Se ve afectada por distintos mecanismos que tratan de obtener nuestra información sin consentimiento, por ejemplo los **spyware** son porciones de código dentro de los programas, diseñados para recolectar información de nuestra computadora y enviarla por Internet en el momento en que nos conectemos.

La solución a este tipo de problemas es tener instalado en la PC un antivirus actualizado y un programa antispyware.

Importante

Los programas que contienen spyware se denominan programas espías porque recolectan y envían a otra computadora información de la máquina en la que se están ejecutando, todo esto sin el conocimiento y consentimiento del usuario afectado.

¡Atención!

Los síntomas del spyware según Wikipedia:
"[...]

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas emergentes (pop-ups), incluso sin estar conectados y sin tener el navegador abierto [...]
- Barras de búsquedas de sitios [...] que no se pueden eliminar.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda más en iniciar el computador debido a la carga de cantidad de software spyware [...]"

Fuente: http://es.wikedia.org, Diciembre 2006

¡Atención!

¡Cuidado!

Muchos de los programas gratuitos que se pueden descargar de Internet contienen spyware. Antes de probar un software es recomendable buscar las opiniones de los usuarios y las críticas especializadas sobre la herramienta.

Correo electrónico no solicitado o correo basura (Spam)

El **spam** es enviado masivamente por las empresas como estrategia de marketing, y la cantidad de mensajes que recibe cada usuario es tan grande que actualmente se ha convertido en una gran molestia para todo aquel que lo recibe.

Definición / Concepto

Spam es el término que se usa para definir al correo electrónico no solicitado que llega a las cuentas de mail de los usuarios.

El problema que se presenta con el correo no solicitado es el espacio que ocupa en las cuentas de correo y el tiempo que le lleva al usuario eliminarlo, por eso los servidores de webmail brindan un filtro automático para detectar este tipo de mensajes, haciendo que un gran porcentaje del spam se almacene en un área de la cuenta de correo que se llama Correo no deseado, en donde los mensajes luego de unos días son eliminados por el sistema.

De todas formas siempre es conveniente revisar rápidamente el asunto de cada mensaje almacenado en Correo no deseado para verificar qué mensajes de nuestros contactos, por error del filtro, se eliminan junto con el spam.

Importante

El spam se recibe en las cuentas de correo, en los mensajeros instantáneos, en los foros, grupos de noticias, y hasta en los celulares. Debido a esta situación muchos países han modificado sus leyes en materia informática para que éstas consideren ilegal el envío masivo de mensajes no solicitados.

¿En qué perjudica a los usuarios el spam?

- Hace perder el tiempo.
- Utiliza espacio de las cuentas de correo.
- Aumenta la carga de trabajo de los servidores que brindan los servicios de correo y mensajería, a raíz de esto los costos de los proveedores se incrementan, impactando en el precio final que debe pagar el usuario.
- La publicidad e información que proviene del spam es de fuente dudosa, por lo tanto carece de utilidad.
- En muchos lugares el spam es considerado un delito.

¿Cómo evitar el correo masivo no solicitado?

La mejor medida es no perder mucho tiempo en este tipo de mensajes y eliminarlos directamente. Muchos se los reconoce solo leyendo su asunto, o incluso por contener palabras típicas del spam como free o gratis.

Como los procedimientos que utilizan las empresas que hacen spam están automatizados, mediante la utilización de programas que van por Internet recolectando direcciones electrónicas de todo tipo, es aconsejable:

- Dar la dirección de e-mail solo a personas que sabemos que harán un correcto uso de ella –amigos, familiares, compañeros de estudio o trabajo, etc–.
- En lo posible no publicar la dirección de e-mail en páginas Web o grupos de noticias.
- En ciertos sitios hay formularios para realizar consultas que solicitan al usuario sus datos personales, no es recomendable completarlos.
- Los mensajes de spam nunca deben ser contestados. Al contestar el mensaje, la empresa que envió el spam estará segura que nuestra cuenta de correo está activa, lo que implica seguir recibiendo más spam.
- Tener instalado algún programa antispam. Este tipo de software se puede descargar libremente de muchos sitios de la Web.

Virus informáticos

Los **virus informáticos** son programas diseñados con el objetivo de causar inconvenientes en las computadoras y en los datos que se encuentran en ella.

Los virus tienen la capacidad de duplicarse y enviarse a sí mismos por medio de distintos dispositivos como un disquete o una red.

La infección a través de Internet es muy factible por el gran caudal de información que se almacena en la Web, por eso debemos tener en claro algunas consideraciones para evitar una infección o saber cómo proceder en caso que la infección ocurra.

Veamos la clasificación de los virus informáticos

Virus de arranque

Se carga en la memoria de la computadora e infecta el sector de arranque del disco. El sector de arranque de un disco es la ubicación donde se encuentra la primera información que lee el SO cuando arranca.

Virus residente

Cuando el virus es residente se esconde en la memoria de la PC y va infectando los archivos o programas a medida que se utilizan.

¡Atención!

Macros en documentos de Word® o Excel®

Cuando recibimos un documento de Office® por correo electrónico hay que tener en cuenta que puede contener una pequeña porción de código –llamada Macro– que tiene la capacidad de ejecutarse en nuestra computadora; por lo que si recibimos un documento que contenga macros de una persona malintencionada podemos sufrir daños en nuestra información.
Los programas antivirus detectan automáticamente los archivos que contienen macros.

Importante

Los daños o inconvenientes que producen los virus son variados: es posible que hagan funcionar lento al equipo, que borren información de los discos o que los programas funcionen de una manera extraña.

Precauciones y solución

Siempre es aconsejable hacer **copias de seguridad** (backup) de los archivos que contienen información importante, así en caso que la computadora se vea afectada por un virus tendrás copias de tu información en un lugar seguro.

Es indispensable tener un antivirus actualizado en la computadora. Existen buenas soluciones gratuitas en la Web. Puedes empezar la búsqueda de un antivirus en: http://www.free.grisoft.com

Actividades

Analiza el siguiente párrafo y emite tu opinión al respecto:

"Al ser software libre, un usuario o empresa puede tomar un programa libre, modificarlo de acuerdo a sus necesidades y venderlo como producto comercial propio."

Trata de responder las siguientes cuestiones:

- ¿Te parece justo que esto sea así? ¿Por qué crees que los creadores del software libre permiten que esto se haga? ¿Crees que de esta manera se logre mejorar el producto?
- ¿Qué diferencias hay entre free software, freeware, shareware, trial y beta?
- ¿Qué es un spyware? ¿En qué nos puede perjudicar?
- Investiga sobre virus informáticos y realiza un informe con el procesador de texto.

Actividades

Lee la nota "Intento de fraude informático en Argentina" y responde:

1. Después de leer la nota que habla sobre un intento de "phishing", ¿qué entiendes por fraude informático?

2. ¿Qué precauciones hay que tener para no sufrirlo?

3. ¿Cómo reaccionan las organizaciones comerciales de nuestro país ante estos hechos? ¿Y en el resto del mundo?

4. ¿Por qué crees que el especialista dice –al respecto del caso tratado en la nota– que el problema no es un tema técnico sino de educación, divulgación y prevención?

NOTICIAS RELACIONADAS

Intento de fraude informático en Argentina

Un periodista de Infobae.com recibió un mail titulado "Atención al cliente de Banca Internet". Luego de explicar una situación muy confusa, se lo invitaba a visitar una página web para completar una planilla con datos confidenciales. El paso a paso del segundo caso registrado en la Argentina

Recibí un mail en la mañana titulado "Atención al cliente de Banca Internet". Como supuse que se trataba de una información de prensa decidí abrirlo. Para mi sorpresa, me trataban como un cliente cuando en realidad no lo soy. Inmediatamente supuse que estaba ante un intento de phishing, es decir robar mi información bancaria.

Primero habría que decir que el hacker que trató de hacer esto es bastante estúpido. ¿Enviarle un mail a una persona que no es cliente de un banco e invitarlo a que complete una planilla? Pero esa es otra historia.

La excusa por la que pretendían que visitara la página web falsa para concretar la estafa es que me había conectado desde diferentes direcciones IP.

Y me decían que si no actualizaba mis datos antes del 28 de abril del 2006 "el sistema informático automatizado de Banca Internet suspenderá su cuenta indefinidamente".

No lo dudé. Me contacté con el banco en cuestión y me dijeron que mi llamado era el cuarto por el mismo asunto y que estaban trabajando en solucionarlo.

Con el actual caso, son dos los que padecen los clientes de bancos locales. El primer intento de phishing lo vivió en febrero una entidad de capitales extranjeros. En esta oportunidad, se trata de un banco argentino.

Es bueno recordar que este tipo de ataques son frecuentes en otros países en donde la banca electrónica está más desarrollada. Sin embargo, el poco tiempo transcurrido entre uno y otro intento de fraude a los clientes locales es un llamado de atención no sólo para las entidades sino también para los usuarios novatos de estos servicios. Vale la pena recordar que entre enero y septiembre del año pasado este delito creció un 688% en Brasil.

Al revisar el primer intento de fraude encontramos que la falsa página web era muy precaria. Pero viendo la imagen del actual intento de phishing encontramos que los hackers están "mejorado" sus tácticas.

Para un usuario novato puede parecer perfectamente normal que una entidad le solicite recargar sus datos por Internet... ¡pero no lo es! Y también, al observar la calidad de la falsa web puede ser que uno caiga en la trampa. Pero cuando chequeamos la dirección web nos damos cuenta al instante que el banco nada tiene que ver con el asunto.

En declaraciones a Infobae.com, Daniel Monastersky, abogado experto en nuevas tecnologías, aseguró que estos casos "van a seguir apareciendo. La Argentina es el único país de la región donde el tema no está instalado. Chile, Brasil, Colombia, todos tuvieron casos importantes. Por eso los clientes de los bancos tienen que sospechar ante cualquier mensaje que les llegue desde un banco".

Cuando se conoció el caso anterior, el experto señaló: "Para combatir esto hace falta educación e información y las empresas en la Argentina no ayudan. En Estados Unidos y en Europa cuando se detecta un caso de este tipo se maneja una política de puertas abiertas y se comunica a los usuarios para que no tengan problemas. Aquí las compañías buscan mantenerlo en silencio para que la gente no desconfíe".

"Esta no es una cuestión técnica: las empresas están bien preparadas con servidores seguros, a nivel técnico la situación está bastante bien, el problema principal es de educación, divulgación y prevención", sostuvo.

Fuente: http://www.infobae.com.ar