Seguridad Informática

En este momento, mientras lee este artículo, un pirata informático podría estar utilizando su ordenador o accediendo a sus datos. Hasta hace muy poco, el ordenador se utilizaba para jugar a videojuegos, escribir cartas, mantener una pequeña base de datos o hacer una hoja de cálculo, pero desde el momento en el que se usa para realizar transferencias bancarias y se ha convertido en un elemento cotidiano clave en nuestro trabajo y en nuestro día a día, el riesgo de que este uso nos pueda causar un grave problema aumenta exponencialmente.

En los últimos años, los virus han evolucionado al mismo ritmo que los ordenadores se han ido introduciendo en nuestras vidas, pasando de ser virus meramente dañinos para las maquinas, buscando ser lo mas notorio posible, causando el mayor daño posible a convertirse en herramientas para cometer delitos.

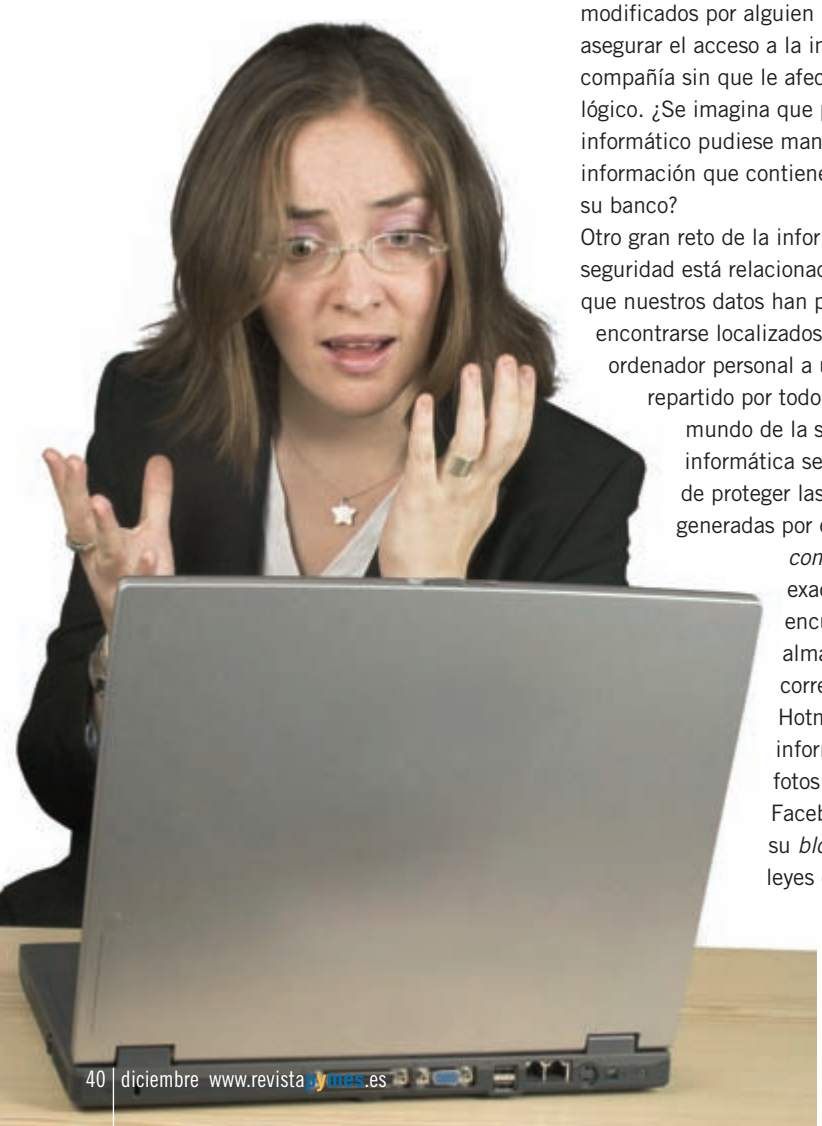
En la actualidad, los mayores peligros de los virus no son sólo los perjuicios que nos puedan causar por la perdida de nuestros datos, hay otros daños mayores como son el espionaje y el robo económico mediante la sustracción de contraseñas y claves, en su mayoría bancarias, pero también de cuentas de correo, con el objetivo de conseguir información personal comprometedora con la que después extorsionan a sus victimas o, simplemente, para suplantar su identidad y con ella cometer delitos en comercios, bancos o empresas.

La denominada Seguridad Informática agrupa las acciones y procesos encaminados a preservar la información contenida en nuestros sistemas por medio de herramientas, acciones y hábitos que buscan preservar su confidencialidad, integridad y disponibilidad.

Debido a la importancia de la informática en nuestra vida actual es importante que todos participemos de forma activa para mejorar la seguridad de nuestra información y de nuestro entorno o cyber-entorno.

La información puede ser afectada de múltiples formas, los aspectos más importantes son confidencialidad —los datos sólo deben ser accesibles por quien está autorizado a verlos— integridad —la información solo debe ser tratada y modificada de forma controlada— y disponibilidad —la información debe ser accesible cuando se la necesita—.

En el entorno privado, las acciones de la seguridad informática pueden ir encaminadas, por ejemplo, a que no se incluyan nuestros datos personales en bases de datos de *spammers* o simplemente a no perder las fotos de las vacaciones o poder acceder a nuestra cuenta de correo.



> ***"No sólo son los usuarios particulares y la información personal el objetivo de estos delincuentes, también es muy codiciada la información perteneciente a compañías o el espionaje industrial"***

Diferentes entornos

En el entorno laboral puede ser algo tan simple y transcendental como que no se divulguen los datos de la nomina de la empresa, que sólo las personas autorizadas puedan ver los datos o documentos relativos a un proyecto de un cliente, que los datos con lo que estamos trabajando son los que deberían ser y no han sido modificados por alguien no autorizado, o asegurar el acceso a la información de la compañía sin que le afecte un fallo físico o lógico. ¿Se imagina que pasaría si un pirata informático pudiese manejar a su antojo la información que contienen los sistemas de su banco?

Otro gran reto de la informática y la seguridad está relacionado con el hecho de que nuestros datos han pasado de encontrarse localizados en nuestro ordenador personal a un entorno virtual repartido por todo el planeta. El mundo de la seguridad informática se enfrenta al reto de proteger las infraestructuras generadas por el *cloud computing*. ¿Sabe exactamente dónde se encuentran almacenados sus correos de Gmail, Hotmail o Yahoo? ¿Y la información personal y fotos que publica en Facebook, en foros o en su *blog*? ¿Conoce las leyes del país que protegen toda esa ingente información acerca de usted?

Actualmente la forma de propagar estos *bots* son cada vez mayores y aprovechan al máximo todas las posibilidades que proporcionan la tecnología con otros fines, convirtiéndose en mas efectivos y potentes como son las redes sociales que se han convertido en autenticas bases de datos organizadas, de las que se puede obtener perfiles completos con fotografías incluidas, hábitos, zona de residencia, costumbres de ocio, ocupación laboral, relaciones sociales, etc... También usan estas redes con millones de visitas y por lo tanto millones de ordenadores potencialmente infectables o convertibles *zombis* para colgar *links* que redirigen a los usuarios a páginas web que automáticamente infectan el ordenador.

No sólo las redes sociales son la forma de llegar a millones de ordenadores, los buscadores mas habituales también son un medio muy efectivo, utilizando paginas con contenidos atractivos para los usuarios como pueden ser eventos sociales muy atractivos y solicitados o la imagen de *celebrities* camuflando en esas paginas contenido activo que intenta infectar la maquina del visitante.

No sólo son los usuarios particulares y la información personal el objetivo de estos delincuentes, también es muy codiciada la información perteneciente a compañías, el espionaje industrial, el acceso a instituciones publicas o causar daños de imagen, manipulando la información contenida en los portales corporativos de las compañías.

Una gran responsabilidad de la seguridad informática se encuentra en nuestras manos y muchas veces podemos encontrar un símil entre la vida real y nuestro cyber-entorno: igual que no acudiremos por curiosidad a un gueto que consideramos peligroso, no debemos visitar páginas web sospechosas, o de la misma manera que no contamos detalles de nuestra vida personal a un desconocido por la calle, no

debemos publicar esa información en sitos web, o igual que no damos la llaves de nuestra casa a cualquiera, no debemos facilitar nuestras contraseñas.

Además de los hábitos de comportamiento debemos adoptar medidas preventivas: si protegemos nuestra casa con una puerta o una alarma, debemos proteger nuestro o sistema con un *firewall*, un antivirus o con las actualizaciones que nos ofrece el fabricante.

Cabe destacar que no estamos solos, existe un Cuerpo Especial de Delitos Telemáticos de la Guardia Civil, cada vez más activo, especializado en la persecución de este tipo de delitos.

En la actualidad no hay un apartado específico de delitos informáticos en el Código Penal, pero sí hay delitos informáticos recogidos cuando los datos o los sistemas informáticos formen parte de la comisión de un delito como son: las amenazas, los delitos sexuales y relativos a la prostitución y corrupción de menores, delitos contra la intimidad, contra el honor, las estafas, el fraude, los daños incluyendo los inmateriales como pueden ser a programas o documentos electrónicos— delitos contra la propiedad intelectual, relativos al mercado y a los consumidores, propiedad industrial u otros.

Consejos

Algunos consejos básicos de seguridad que debemos observar son los siguientes:

• Mantener actualizados nuestros sistemas informáticos mediante las funciones que nos ofrecen los fabricantes de los mismos, algunos mediante acciones manuales y otros que se pueden automatizar mediante herramientas que ofrecen los sistemas. Esta práctica es especialmente recomendable para los sistemas operativos y navegadores de Internet.

• Trabajar con cuentas de usuario que tengan los menos privilegios posibles. Un gran error cometido habitualmente es la utilización de un usuario con privilegios de admitrador, ya que un perfil de administrador infectado podría acceder a toda la información contenida en ese ordenador, pero si pertenece a una red también podría acceder al resto de maquinas cercanas.

• Utilizar antivirus y mantenerlos actualizados. Este tipo de herramientas de seguridad normalmente son actualizadas en remoto y automáticamente por el propio fabricante del mismo.

• Utilizar programas *firewall*, los hay de muchos tipos: desde maquinas muy sofisticadas, que se utilizan para proteger redes de corporaciones, hasta sencillos programas gratuitos, todos son muy efectivos y recomendables.

• No leer mensajes de correo electrónico procedentes de direcciones desconocida. No debe leerlos y, por supuesto, no deben reenviarse.

• Hay que tener especial cuidado con los archivos descargados de redes P2P, ya que son un medio habitual para la distribución de virus y *malware*.

• Buscar páginas de Internet de confianza, preferiblemente selladas por certificados y formas digitales.

• Utilice siempre software legal. Evita las descargas de programas de lugares no seguros de Internet.

• No fomentar las cadenas por Internet, se aprovechan de la buena fe del usuario para que reenvíe el correo a sus conocidos y, de esta manera, captar direcciones de correo electrónico para prospectivas comerciales.

• Desconfíe de los mensajes de correo procedentes de supuestas entidades bancarias.

• Confirme vía telefónica, en su sucursal bancaria, cualquier petición que reciba de datos de banca electrónica.

• En las redes sociales, limite el acceso de la información que comparte a personas conocidas —mis amigos—. Cuanto más amplio sea el círculo de contactos —amigos de mis amigos y todos los usuarios—, a más riesgos se expone.

LA ADOPCIÓN DE ESTAS MEDIDAS NO GARANTIZA LA SEGURIDAD DE NUESTROS SISTEMAS PERO REDUCE EN UN 90% SU VULNERABILIDAD.

En definitiva, lo que debemos tener en cuenta es que gran parte de la Seguridad de nuestra información se encuentra en nuestras manos como usuarios.

Stéphanie Haye
Grupo SCA

"Existe un Cuerpo Especial de Delitos Telemáticos de la Guardia Civil, cada vez más activo, especializado en la persecución de este tipo de delitos"