

DÍA DE LA SEGURIDAD EN INTERNET 2010

Navegación segura, confianza en línea para tod@s

El nivel de seguridad asociado a un sistema corresponde al nivel de seguridad de su eslabón más débil, y el eslabón más débil de un sistema informático es casi siempre el usuario. Así que si queremos movernos en Internet con seguridad, deberemos dejar la pereza de lado y ser algo más protagonistas y conocedores del sistema informático que usamos.

Antivirus sí, pero...

no caigas en la falsa sensación de seguridad que pueda proporcionarte. Los antivirus sólo son efectivos contra los virus ya conocidos, no contra los nuevos que vayan apareciendo, hasta que éstos hayan sido detectados, analizados y añadidos a la base de datos del programa en sucesivas actualizaciones. Por lo tanto, si tienes antivirus es necesario actualizarlo con frecuencia. Afortunadamente los antivirus ya permiten que deleguemos en ellos la tarea de descargar las actualizaciones, y si son diarias mejor que mejor.

Firewalls, el siguiente nivel

tampoco esta protección es perfecta; de hecho, los cortafuegos pueden esquivarse en ocasiones, pero es un factor más que puede ayudarnos a determinar si tenemos algún tipo de software malicioso en el ordenador. Si de pronto el cortafuegos nos avisa de que un programa quiere conectarse a un puerto determinado de otro ordenador y no conocemos ese programa, puede que estemos ante el intento de un troyano recién instalado de comunicarse con otros ordenadores.

Nunca guardes tus claves en el propio ordenador

Cada vez son más los sitios de Internet donde se requiere tener una cuenta, con nombre de usuario y clave. Desde el correo electrónico y los bancos al messenger, las redes sociales e incluso algunos foros que exigen identificarse antes de poder participar en ellos. En consecuencia, el número de claves a recordar se va haciendo para muchas personas casi inmanejable. No es necesario ser una persona de avanzada edad para tener ya problemas a la hora de memorizar multitud de claves. En consecuencia, muchas personas optan por apuntar las claves difíciles de recordar, si no todas. No está de más insistir en que, en ese caso, deben apuntarse en papel y no dejar nunca ese "libro de claves" a la vista o en las cercanías del ordenador. Por supuesto, nunca jamás deben almacenarse en un fichero en el propio ordenador. En caso de que perdamos el control del mismo debido a algún virus o troyano o bien si nos roban el equipo o lo perdemos, habremos dado a la persona que lo tenga la posibilidad de acceder a todos nuestros datos (posiblemente hasta los bancarios)

¿Qué hacer si lo que nos roban es el propio equipo informático o lo perdemos?

Aparte de la evidente acción de denunciar ante la Policía su sustracción o pérdida, debemos pararnos a pensar qué información hemos dejado al descubierto y actuar en consecuencia. Los navegadores y el resto de programas que interaccionan con Internet permiten darnos la opción de

recordar la clave por nosotros -para evitarnos teclearla una y otra vez- y permiten también que inicien sesión automáticamente de forma que ni siquiera tengamos que introducir el nombre de usuario. Esto es muy cómodo en situaciones normales pero se vuelve un problema serio de seguridad si ese ordenador cae en manos ajenas, puesto que permite que nuestra identidad sea suplantada en multitud de sitios sin ni siquiera necesitar nuestras claves de acceso.

Por tanto, en una situación así necesitaremos cambiar de inmediato todas las claves que hubiéramos almacenado en ese ordenador, a fin de retomar el control de nuestras cuentas antes de que lo haga quien tenga el ordenador en su poder. Y si el ordenador perdido era el único que teníamos deberemos recurrir a algún familiar o amigo de confianza para que nos permita usar su equipo para modificar esas claves lo más pronto posible.

Compras por Internet

Ante el crecimiento del comercio electrónico, cada vez nos enfrentamos más al dilema de pagar con tarjeta en Internet. Una opción a tener muy en cuenta es la de abrirnos una cuenta bancaria secundaria y específica para las compras por la Red con una tarjeta de débito asociada a ella. De ese modo podemos mantener un saldo bajo pero suficiente para las compras que solemos hacer. Con cierta periodicidad, o poco después de realizar la compra o poco antes de la siguiente, si es que podemos planificarla, bastará con "recargar" la misma con una cantidad similar a la gastada para mantener el nivel de saldo de esa cuenta. Si realizamos compras por Internet, seguramente también usaremos la banca electrónica con lo cual bastarán unos cuantos clicks para transferir esa cantidad desde nuestra cuenta corriente principal. Esto tiene una ventaja añadida, ya que ayuda a controlar nuestros gastos. Una compra por Internet es fácil y rápida, y muchas veces no somos conscientes de cuánto hemos gastado. Mediante este sistema, nos obligamos de alguna manera a fijarnos también en lo que nos hemos gastado y si superamos el presupuesto que nos podamos permitir en cada momento.

Los dominios en Internet y el Phishing

Debemos fijarnos siempre (especialmente en el caso de la banca electrónica) en la barra de direcciones del navegador para ver si estamos realmente en el sitio que creemos estar. La parte fundamental de la dirección es siempre lo primero que aparece a la izquierda del tipo de dominio (.com, .net, .es, etc) Por ejemplo, <https://extranet.banesto.es> sería una dirección válida para la entidad Banesto (lo primero que se encuentra a la izquierda del .es) .Sin embargo, si viéramos <https://banesto.extranet.es> estaría claro que no estaríamos en la página de esa entidad (en este caso, el dominio sería extranet, no banesto). Incluso si viéramos <https://banesto.aa.es> estaríamos ante un más que probable intento de phishing (el dominio en este caso sería "aa")

En cuanto a las claves de acceso a la banca electrónica nunca nos cansaremos de recordar que un banco jamás las pedirá a sus clientes, de hecho ni siquiera son conocidas por los empleados de nuestra sucursal habitual. Si alguien intenta conseguir nuestras claves bancarias, tratará de poner a prueba nuestra capacidad de confianza en el interlocutor de múltiples maneras; por tanto, lo mejor que se puede hacer en una situación así es colgar el teléfono de inmediato y no dar siquiera la oportunidad de que acaben por convencernos.

Lo mismo se aplica para las tarjetas de coordenadas. Los bancos nos solicitarán las coordenadas para algunas operaciones, pero nos pedirán una sola coordenada por operación, dos a lo sumo, para verificar que somos quienes decimos ser. Si una página que parece ser la de nuestro banco nos pide

más coordenadas o incluso todas, estaremos sin duda ante una página falsa. No prosigas con la operación y cierra el navegador. Para mayor tranquilidad puedes consultar en tu sucursal bancaria el número de coordenadas que te solicitarán.

¿Aceptarías como trabajo traer cocaína desde Suramérica a España oculta en tu cuerpo? Entonces, tampoco aceptes el scam para desviar fondos.

La única recomendación vuelve a ser usar el sentido común, nuestro mejor aliado para protegernos en la Red. Como reza el dicho, nadie da duros a cuatro pesetas. Si nos ofrecen un trabajo desde casa para el que sólo necesitamos una conexión de Internet y unos pocos minutos al día con el cual podemos ganar muchísimo dinero al mes sin hacer prácticamente nada, estaremos seguramente ante una estafa de trabajo falso o "scam". Lo más habitual es que traten de captarnos como "muleros", al estilo de los que trasladan droga. En este caso, lo que se trata de trasladar es dinero, de procedencia más que dudosa. El "empresario" nos ofrece una comisión para que nosotros realicemos las transferencias. Mientras no se descubre, él consigue desviar fondos a otro país a cambio de la pequeña comisión que nos ofrece. Cuando se descubre, la policía te detiene a ti por ser el autor de las transferencias. En ambos casos, él gana y tú pierdes, siempre.

El caso de los adjuntos extraños

Muchas veces podemos encontrarnos mensajes de correo que nos impulsan a abrir un fichero adjunto al correo insistiendo en que es muy bueno, muy importante o muy divertido. Si no conocemos al remitente, lo mejor que podemos hacer es ignorar la sugerencia y borrarlos directamente. Si lo conocemos (un amigo, por ejemplo) pero nos extraña la forma de escribir y no estamos seguros de que sea suyo, lo mejor que podemos hacer es confirmar con esa persona que ha sido realmente la que nos ha enviado el mail antes de abrirlo. Incluso si estamos prácticamente seguros de que esa persona nos ha enviado el mail con el adjunto debemos pasar siempre el antivirus a ese fichero (nuestro amigo puede haber reenviado el mail a sus contactos antes de abrirlo y haber transmitido un virus o troyano inadvertidamente)

Finalmente, siempre debes fijarte en el nombre del archivo adjunto. Si contiene dos extensiones en lugar de una (se llama por ejemplo: leeesto.txt.vbs en lugar de leeesto.txt) no lo abras bajo ningún concepto y bórralo inmediatamente, lo más probable es que se trate de un virus o un troyano "camuflado" como si fuera un archivo inofensivo.

Más información sobre seguridad:

- [Noticias sobre seguridad](#)
- [Seguridad en la Red](#)
- [Seguridad Pymes](#)

10 consejos que los menores deben conocer para no caer en la Red.

En el especial caso de los menores y, además de los dispositivos que la tecnología pueda ofrecer,

para evitar que sean víctimas de la Red, debe insistirse en la precaución como escudo por excelencia: evitar que se muestren sin límites en Internet, que tengan en cuenta el alcance que puede tener cualquier tipo de información que sea insertada en Internet. Como precauciones generales, debe insistirse en la educación

- 1.- Internet retiene todo rastro de tráfico, la información que transporta puede ser rastreada.
- 2.- Internet es un sistema de comunicación utilizado por personas: precaución y respeto por quién está al otro lado.
- 3.- Internet se parece a la vida física más de lo que creemos, desconfía de aquello que te haría desconfiar en la calle (por ejemplo, la imagen de una tienda o la personalidad de un desconocido).
- 4.- Internet es información, para saber si es o no útil, si es o no verdad, siempre debe ser contrastada. Solicita consejo a un adulto de confianza antes de actuar.
- 5.- Internet dispone de todo lo que insertamos en sus redes, debemos evitar ofrecerle demasiada información sobre nosotros mismos, y ser conscientes de lo fácil que es perder el control sobre ello.
- 6.- Internet no es ilegal, pero puede ser el escaparate de la comisión de un delito, estate atento a lo que te llega a través de sus redes y, desconfiar de lo que tenga un origen incierto.
- 7.- Internet es paralela a la vida real, no ajena, lo que en ella ocurre suele tener un reflejo directo en el ámbito personal y físico de los implicados.
- 8.- Internet permite manejar dinero sin necesidad de tocarlo, las transacciones que realices, que sean con permiso seguro del banco en que confías. Desconfía de los envíos de dinero que no pasan por una entidad bancaria o una administración pública estatal.
- 9.- Internet pone a nuestra disposición más datos de los que podemos asumir y, de la misma forma que ocurre en la vida real, necesitamos filtrar aquello que sobra para un desarrollo personal pleno, ya sea con el sentido común, ya lo sea con ayuda de dispositivos técnicos de filtrado.
- 10.- Existen leyes que castigan las actividades ilícitas en Internet, y también existen leyes que protegen a sus usuarios de una mala utilización de Internet, especialmente cuando afecta a sus derechos fundamentales (intimidad, secreto de las comunicaciones, datos personales, libertad de expresión, etc.). Si eres víctima denúncielo.

[La Asociación de Internautas necesita tu ayuda](#)

También puedes donar enviando un SMS:

Desde España enviar AI al 27595 (Coste 1,20 euros + IVA)

Servicio especial de donaciones gracias a [SEPOMO Micropagos](#)

Fecha artículo: 2010-02-09 06:01:58 - url artículo: <http://www.internautas.org/html/6006.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2010 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org