



Consejos Básicos de Seguridad Contra el Fraude On-Line

Es necesario partir de la siguiente premisa "La Seguridad Total No Existe", a resultas de esta máxima, la única herramienta eficaz de la que disponemos es la información y la prevención, por ello, aquí os dejamos unos consejos básicos fundamentales para desenvolverse en la red de redes.

Lo primero y fundamental es tener nuestro ordenador actualizado, es decir, tener instaladas las últimas versiones del sistema operativo y navegador web, también es muy recomendable hacer uso de un buen programa antivirus junto con un cortafuegos y actualizarlos frecuentemente, estas medidas solucionan gran parte de las vulnerabilidades de nuestros ordenadores.

Comercio Electrónico y Compras en Línea

Antes de realizar cualquier compra en línea asegúrese de que la empresa vendedora dispone en su página web de una pasarela de pagos segura, las direcciones web donde se introduzcan datos personales y de pago deben comenzar por "*Https://*" y debe aparecer un dibujo de un candado en su navegador.

No acepte pagar en ningún caso por ningún tipo de servicio de envío de dinero, pues este no sería nunca el método de pago empleado por una empresa seria.

Compruebe que en la website de la tienda on-line figuran los datos fiscales de la misma, así como su sede social y formas de contacto.

Truco Haga una búsqueda en internet con el nombre de la tienda, seguramente obtendrá muchos resultados, si la mayoría son negativos, desconfíe ;

Si va a realizar la compra a un particular, con el que ha contactado por medio de un foro o una página de compra-venta, tenga en cuenta lo siguiente:

Es importante saber con quien se trata, reúne todos los datos posibles, si vas a pagar por transferencia bancaria, solicita a tu banco un recibo y no olvides poner el concepto exacto y el destinatario.

Desconfíe de los anuncios de venta donde se ofrecen productos de alto valor a un precio muy por debajo del mercado, sobre todo si se le solicita que ingrese o envíe una cantidad de dinero como señal, no lo haga ;

Acabar con el Fraude es cosa de ToDoS, No Caigas en la Trampa ;

<http://www.fraudeenred.com/>



Si vas a pagar contrareembolso debes saber que algunas agencias de mensajería permiten la apertura del paquete antes del pago, esto es algo en lo que deben estar de acuerdo comprador y vendedor, pues es un servicio extra y como tal hay que solicitarlo.

Procure guardar copias de todo, anuncio de venta, mensajes privados, mensajes de correo, direcciones de correo y de la web donde se anunciaba.

Muy Recomendable

Un método muy recomendable y que nos puede ahorrar más de un susto, consiste en disponer de una cuenta bancaria y una tarjeta de débito asociada a esta, que utilizaremos exclusivamente para nuestras transacciones en internet.

De esta manera, en dicha cuenta solo dispondremos del efectivo suficiente para estas operaciones y aunque nuestros datos cayeran en malas manos, no podrían obtener ningún beneficio.

Phising y derivados

Debe tener siempre presente, que ni su banco, ni su ISP o cualquier otro servicio le pedirán nunca por mail que por motivos de seguridad, administración o cualquier otro, introduzca sus datos personales.

Siempre que desee acceder a cualquier servicio bancario on-line abra una ventana nueva de su navegador y teclee personalmente la dirección del mismo, jamás lo haga mediante enlaces o hipervínculos que reciba por mail o vea en cualquier otra web.

Asegúrese de encontrarse en un servidor seguro y que la dirección que vea en la barra de direcciones sea la que corresponde con el sitio oficial de su entidad, las direcciones de servidores seguros deben comenzar por "Https://" y tiene que aparecer un dibujo de un candado en su navegador.

A Tener en Cuenta:

- No introduzca ningún dato en los formularios de los que desconozca su origen.
- No haga click con su ratón en los enlaces bancarios recibidos por e-mail.
- Asegúrese de estar en un servidor seguro antes de realizar cualquier operación.



E-mail, Scam y Hoaxes

Desconfíe de cualquier mensaje que reciba de remitente desconocido, por muy sugerente que le resulte el asunto, lo mejor que puede hacer es borrarlo directamente.

Tenga cuidado con las ofertas de trabajo que reciba por email, principalmente de aquellas que ofrecen condiciones muy ventajosas, habitualmente se le ofrecerá que gestione a través de sus cuentas ciertas cantidades de dinero, por las que usted se quedarán un porcentaje, esta es una versión moderna del timo de "Las Cartas Nigerianas" y con ello usted esta blanqueando dinero procedente de actividades ilícitas y por lo tanto, cometiendo un delito.

Procure no caer en la tentación de reenviar los mensajes en cadena, conocidos como HOAX, pues solo conseguirá perjudicar y congestionar los servidores de correo, así como facilitar una gran base de datos de cuentas de correo al autor que habitualmente son vendidas y usadas para el envío de mensajes de publicidad no deseados, conocido como SPAM.

Dialers

Este tipo de fraude actualmente solo afecta a los usuarios que se conectan a internet por medio de un modem 56k, marcando el número del nodo en cada conexión.

Es muy importante tener cuidado con los sitios web por los que navega y sobre todo con los archivos que descargue de webs desconocidas.

Compruebe frecuentemente su configuración de red, para verificar si los datos siguen siendo correctos.

Elimine cualquier conexión nueva que aparezca en su acceso telefónico a redes que usted no haya creado personalmente.

Afortunadamente la mayoría de los antivirus actuales detectan y eliminan este tipo de programas, es por esto que le recomendamos una vez más que disponga en su ordenador de un antivirus actualizado.

Consideraciones Finales

Esta es una pequeña guía orientativa para poder protegerse de forma más efectiva en la red, no obstante la mejor herramienta es el propio sentido común y la experiencia.