

Cómo prevenir el robo de datos en internet



Hoy os hablaré de uno de los problemas de seguridad más serios de internet: El robo de nuestra información personal y la suplantación de identidad.

Pero empecemos con un poquito de humor.

Sofocleto decía en sus sinlogismos: La ignorancia consiste en saberlo todo, pero de otro modo.

Por desgracia, en internet, la ignorancia puede salirnos muy cara. Cada día es más frecuente recurrir a internet para realizar compras, consultar nuestros datos bancarios, comunicarnos con la administración, etc..

Y, a pesar de que mucha gente ya está utilizando las nuevas tecnologías para realizar estos trámites, pocos siguen unas mínimas normas de seguridad para evitar posibles problemas.

A nadie se nos ocurría salir a la calle con 100.00 € y llevarlos colgados de la mano en una bolsa transparente ¿verdad?. Pues mucha gente, sin saberlo, está haciendo eso

mismo en internet.

Para hacerse con nuestros datos, los hacker se sirven de unos programas llamados keylogger , que son un tipo de programa espía cuya función es capturar las pulsaciones de nuestro teclado y guardar esa informa en ficheros de texto que son enviados al hacker en cuestión.

Estos programas maliciosos suelen llegar a nuestro ordenador «disfrazados» de programas que hacen otras cosas o «escondidos» dentro de un correo electrónico o de un programa pirata. Esta habilidad que tienen de esconderse dentro de otra cosa hace que también se les suela conocer con el nombre de troyanos

De este modo, una vez infectado nuestro ordenador con este tipo de virus, TODO lo que escribamos (cartas, correos, claves del banco, contraseñas, cuentas corrientes, etc... pasará a estar en poder del hacker que ha diseñado el programa espía, quien podrá usar tranquilamente la información robada.

Si, por ejemplo, accedemos a nuestra cuenta bancaria, la persona que ha interceptado nuestras comunicaciones recibirá algo como esto:

```
http://www.santander.com/cuentasbanco <enter >alfredo <enter>
Arc45T44 <enter>
```

La página web del banco, vuestro nombre de usuario y vuestra contraseña. Ni mas ni menos. Y da igual si el banco tiene una página web con conexión segura, o si codifica los datos antes de enviarlos. El virus actúa ANTES de que entren en funcionamiento estas medidas de seguridad, así que resultan ineficaces.

Pero no nos pongamos paranoicos, por suerte contamos con algunas herramientas para neutralizar este tipo de virus.

La más conocida de todas es KeyScramble, de QxfSoftware.

Keyscramble se encarga de encriptar todas las pulsaciones del teclado a nivel interno de windows, de manera que cuando la información es capturada por el key logger ya se encuentra encriptada. Posteriormente, cuando los datos llegan a la aplicación, se desencriptan, quedando así a salvo de miradas indiscretas.

Existen tres versiones distintas del programa:

– Gratuita: Sólo es capaz de proteger los datos enviados los navegadores web más utilizados (explorer, chrome, firefox, safari, etc...). Esta versión cubre los niveles mínimos de seguridad para cualquier usuario, ya que nos protegerá de cualquier intento de acceder a nuestra información cuando usamos la página web de una tienda online, nuestro banco, etc...

– Profesional: También nos protege cuando utilizamos otro tipo de programas que no son un navegador web, como programas gestores de contraseñas, email, editores de texto, etc... Tiene un precio de \$29.99 y se puede instalar en 3 ordenadores

– Premium: Además de todos los programas anteriores, protege también software financiero, Dropbox, Google drive, el explorador de archivos de Windows, etc... Tiene un precio de \$44.99 y se puede instalar también en 3 ordenadores.

En resumen: cuando menos, todos deberíamos tener instalada al menos la versión gratuita. Las otras dos versiones también son recomendables y como podéis ver, tampoco tienen un precio demasiado elevado, sobre todo si podéis aprovechar la licencia múltiple; ya que en ese caso la versión premium os saldrá a menos de 15 euros por ordenador.

Como todo en esta vida, nada es infalible, y aún contando con estas herramientas podemos estar en peligro, pero al menos no saldremos a la calle con el dinero en una bolsa transparente.