

Internet básico. Seguridad básica II.
“¿Por qué no puedo cambiar la página de inicio?”

Basic Internet. Basic Security II.
“Why I can't change my home page?”

Spywares, Adwares, Hijackers, Spam y otros bichos... un mal ¿necesario?

Bien. En la primera parte vimos como nosotros usuarios les ponemos la mesa a aquellos que se dedican a molestar gente en la red.

Cuántas veces hemos oído: “¡no puedo cambiar mi página de inicio!”, “¿de donde sale esa publicidad?”, “¿por qué hace eso mi Güindous?”, “¿quién me mandó toda esa información que yo no pedí y no me sirve?” y otras tantas mas.

Bueno, aunque parezca increíble nosotros mismos hemos permitido que todo eso pase.

Spyware, Adwares, y hijackers.

Muchos de los causantes de esos problemas son los “spywares”, “hijackers”, y los ahora llamados “adwares” (Advertisement software, o software de publicidad).

¿Qué es spyware/adware? Sucede que NUNCA NADA en internet es GRATIS. NUNCA.

Cuando bajamos algún programa de la red “gratis” resulta que puede no venir solo.

¿De verdad creen que alguien puede desarrollar un programa para que se use completamente gratis? Si ni en Linux sucede =P (de no ser que algún programa se sujete a la licencia GNU/GPL difícilmente puede ser verdaderamente gratuito).

¿Cómo hacen dinero entonces si no pagamos por el programa?

Con publicidad, empleando Spywares/Adwares.

Un SPYWARE es un programa que se dedica a monitorear nuestra actividad, en especial lo que hacemos en internet: qué sitios visitamos, qué tipos de temas acostumbramos en internet, cuanto tiempo pasamos en la red, quién nos envía correo, a quién le enviamos correo, y todo ese tipo de información. La información recolectada es enviada a algún lugar en internet donde es analizada y comercializada.

Un ADWARE es un programa que dependiendo de nuestra actividad en la red en tiempo real nos hace llegar publicidad ya sea por pop-ups o por correo electrónico.

Y los HIJACKERS (secuestradores) son programas o agregados que pueden ser parte de algún spyware/adware y se encargan de modificar el comportamiento de nuestra maquina “forzando” a usar páginas de inicio, de búsqueda y de error que son parte del software que lo haya instalado.

Tal vez ya empiecen a verle forma a este asunto.

Para empezar hacen que nuestras maquinas funcionen de manera rara. Cambian la página de inicio, cambian la página de error, muestran información rara o que no deseamos, abren ventanas inesperadamente, hacen que nos lleguen correos electrónicos que no deseamos, y cosas por el estilo.

Luego, estos programas casi siempre se instalan de manera oculta, sin avisar, incluso por ese comportamiento se les puede considerar como troyanos.

Para seguir, yo creo que a nadie nos gusta que nos estén vigilando, es una vil violación a la privacidad. Es como ir desnudos por la internet y bajo una lupa.

¿Qué podemos hacer?

1. ANTES de instalar CUALQUIER programa bajado de internet es bueno investigar referencias de ese programa. Nada mejor para este fin que el buen Google. Casi siempre que se descubren spywares relacionados a algún programa se propaga la noticia en la red. Dependiendo de lo que averigüemos acerca de ese programa podremos decidir si lo instalamos o no. Por ejemplo, les puedo citar de antemano que iMesh ver. 3.0 o Kazaa ver. 2.6 tienen unos spywares MUY AGRESIVOS. Por fortuna para todo hay alternativas, si de p2p se trata, un buen sustituto de Kazaa es el Kazaa Lite... y toda esa información la pueden averiguar en la misma internet.

El proceso de instalación y funcionamiento de un spy/ad/hjck puede ser muy complejo. En muchos casos están vinculados el software que lo instala y el spy/ad/hjck, de tal forma que sin el complemento publicitario el programa no funciona. ¿Qué hacer en esos casos? Podemos recurrir a

2. Herramientas especializadas en remoción y prevención de spywares, adwares y hijacks. Las tres principales que recomendaremos por ahora son el CWShredder ([click aquí para saber mas](#)), el Hijackthis ([click aquí para saber mas](#)) y el Spybot Search & Destroy ([click aquí para saber mas](#)).

Curiosamente, existe un sutil riesgo. Les recomiendo que antes de utilizar una herramienta antispyware/antiadware/antihijackers que no sea alguna de las que les mencione también investiguen referencias al respecto de ellas, porque resulta que por ahí hay muchas herramientas que quitan unos spys/ads/hjck.... y dejan los suyos =P

Curiosamente, estos programas (los spys, ads y hjcks) no han hecho más que automatizar una muy vieja herramienta de comercio que existe aun desde antes que la Internet... los correos cadena, ahora también llamados "spam".

Los correos cadena y el spam también son una amenaza importante para la privacidad y la seguridad. Si bien a diferencia de una cadena de correos un spyware, adware, o hijacker, funcionan de manera automática y masiva, el riesgo es parecido.

Ojo. Es necesario hacer una importante diferenciación. No es lo mismo spam que una cadena de correo aunque al final resultan igual de molestos.

Las cadenas de correo son mensajes que EL MISMO USUARIO PROPAGA.

El spam es información que llega... no sabemos de donde, no sabemos por qué, no sabemos cuando... pero llega.

Cadenas de Correo.

¿Cómo nos perjudica una cadena de correos? Simple. Casi siempre son iniciadas por empresas que se dedican a la publicidad. Entre mas gente participa en la cadena, mas direcciones de correo recolectan esas empresas. Entre mas direcciones de correo recolectan esas empresas mas posibilidades tienen de hacer llegar su publicidad. Y es efectiva porque de antemano saben las empresas que si una dirección de correo se anexó a la cadena es porque esa dirección de correo existe, esta en uso, y hay alguien que la revisa de manera regular.

Cada dirección de correo electrónico anexada a una cadena es dinero contante y sonante para las empresas y es una sentencia a seguir recibiendo BASURA en el correo. Y a ti ¿cuántos correos que no deseas te llegan a tu buzón? Bueno, pues de la mayoría de ellos tu mismo puedes tener la culpa de recibirlos.

¿Cómo prevenimos las cadenas? NO PARTICIPANDO EN ELLAS. No es verdad que Bill Gates va a regalar dinero por probar su seguridad, no es verdad que Mercedes Benz va a regalar un auto por probar su sistema, no es verdad que Nokia va a regalar teléfonos, no es verdad que la Coca-Cola a partir de cualquier fecha se va a volver peligrosa, no es verdad que existe un niño@secuestrad@, no es verdad que existen inversionistas buscando tu ayuda, ¡NO ES VERDAD NADA DE ESO! ¡NADA!

Tampoco es verdad que si envían 30,000 correos les va a ir mejor, o que si no envían 200,000 les va a caer una maldición. ¡NO ES VERDAD!. Es importantísimo que tomemos conciencia real del daño que le hacemos al internet y a nosotros mismos participando en estas cadenas.

Existe una estimación, de que por cada cadena que respondemos nos llegan de 7 a 8 correos DIARIOS que no deseamos.... Piénselo.

¿Cómo prevenimos el spam? La regla de oro. Nunca abran un correo que no sepan quien se los envió. ¡NUNCA! ¡Y mucho menos lo respondan!

Además, suponiendo que ya recibieron 25,000 veces el mismo mensaje y ya los tiene cansados, de todas formas no lo abran. Mejor intenten bloquear la dirección de donde lo envían. El famoso link para remover es casi como responderle al spam. Si usamos el famoso link que se usa "para que no sea considerado spam" es una manera de avisar al emisor que esa dirección de correo esta vigente y que alguien la revisa regularmente, lo que es mantener vigente nuestra dirección para ellos.

Si bien mantener "limpia y segura" nuestra dirección de correo electrónico es prácticamente imposible, si podemos tomar la responsabilidad de no causar ni causarnos más problemas.

Haciendo un rápido resumen: si tu maquina se porta raro y te aparece información que no sabes de donde viene puede ser un spyware, un adware, y/o un hijacker, basta con utilizar el CWSHredder, el Hijackthis y/o el Spybot Search & Destroy; 0 respuestas o participación a las cadenas, y 0 respuestas a los spams. Simples consejos que les harán la vida en la red un poco más segura y tranquila.

Ahora ya saben porque esos skins, esos punteros para el ratón, esos iconos para el correo, esos p2p, esos programas para untarle jalea al pan, etc etc etc, son "gratis" y porque es preferible... no instalarlos.

Breviario cultural xD

¿Por qué se le llama spam a la basura en internet?

No nos complicaremos mucho en cuanto a fechas. A grandes rasgos es que en el transcurso de la Segunda Guerra Mundial y las posteriores guerras como la de Vietnam el ejército estadounidense incorporo como parte de la dotación de campaña para sus soldados un alimento: el Spam. El Spam es una carne fría enlatada, un como trocito jamón que se presenta en una lata abre fácil. Un alimento fácil de llevar a cualquier lugar, sin necesidad de condiciones para conservarlo, y fácil de comer. Y sucedió. Como en muchos productos militares, fueron tocados por la mano de la mercadotecnia y el Spam paso al consumo del público en general.

Pero también como sucede con muchos productos, no tardo en aparecer sus comentarios negativos. En primera se puso en juicio el contenido de químicos necesarios para usarse como conservadores. Si bien estoy enterado, el spam tenía muy altas cantidades de yodo. En segunda, se puso en juicio su sabor: o lo amaban o lo odiaban, pero a nadie dejaba indiferente.

A pesar de eso, el spam era (y es todavía hoy día) un fenómeno de ventas. De hecho fue un alimento precursor de una nueva generación de alimentos conservados y los métodos de prepararlos.

¿Y que tiene que ver eso con la basura de la red? Bueno, resulta que en su mayor época de auge el Spam era encontrado en todas las comidas, vaya, se decía que hasta en restaurantes finos había alimentos que de una u otra forma incluían Spam.

Así que se formo una frasecilla por parte de a quienes no les agradaba el spam:

"Spam es esa molesta carnecilla que esta en todos lados y no sabes como deshacerte de ella".

Posteriormente lo que se hizo fue pasarla al ambiente de la internet:

"Spam son esos molestos mensajes que están en todos lados y no sabes como deshacerte de ellos".

Contáctanos si necesitas ayuda u orientación, estamos para servirte:

Ahoraybien.com
e-mail informes@ahoraybien.com
website <http://www.ahoraybien.com>
Tel. directo (0155) 5837-1707
Fax (0155) 5837-7208
Cel. 04455-1191-3202 y 04455-5456-7271