

Outpost Firewall Pro para el usuario final

Amenazas en Internet

Una calle de dos vías

Aunque Outpost protege a su ordenador con sólo instalarlo, es útil saber cómo funciona. Para comprender cómo y por qué existen las amenazas en Internet, es importante comprender cómo está organizada. Internet es una red de redes que interconecta a millones de ordenadores entre sí.

Es esencial saber que no existe diferencia entre ordenadores utilizados en el hogar, servidores corporativos y sitios de Internet en lo que concierne a cómo cada cual envía y recibe señales electrónicas. Cualquier ordenador en la red envía y recibe datos.

Cualquier ordenador puede solicitar una conexión con otro ordenador, incluyendo el suyo.

Internet es realmente una calle de dos vías donde los datos, incluyendo los comandos, se trasladan desde y hacia su equipo.

Esto presenta la conclusión obvia: conectarse a Internet permite que muchas personas malintencionadas puedan llegar a su ordenador personal, si el mismo no está protegido.

Conozca al enemigo

Para protegerse contra potenciales amenazas es mejor conocer al enemigo y sus hábitos.

Estas son las amenazas más comunes en Internet que los usuarios personales deberían tener en cuenta:

Amenaza	Riesgo potencial
Intento de intrusión	Acceso no autorizado a su ordenador (control total de su sistema y de todos sus archivos)
Virus y ataques remotos	Pérdida de sus datos (archivos y documentos), interrupciones del sistema, funcionamiento inestable del ordenador
Troyanos	Acceso no autorizado a su ordenador (control total de su sistema y todos sus archivos)
Páginas maliciosas en Internet	Pérdida de su privacidad
Programas espía	Pérdida de su privacidad

Sin una protección adecuada, su ordenador está abierto a todas estas amenazas.

En la actualidad, las herramientas de los agresores informáticos son muy fáciles de utilizar, incluso para quienes no tengan grandes conocimientos.

Por consiguiente, hasta los niños podrían utilizarlos por las más diversas razones: desde la simple diversión, o la vanidad de espiar datos confidenciales, hasta el intento delictivo de hurtar los datos personales o el dinero de un usuario.

Las consecuencias de cualquiera de los ataques mencionados pueden ir más allá de simplemente perder, por ejemplo, el fichero Mis Imágenes.

Pueden producir el formateo total de su disco duro, eliminando todos sus archivos y programas. Incluso, el usuario desprotegido se expone al hurto de las claves de su tarjeta de crédito, de su cuenta bancaria, o de otros datos confidenciales almacenados en su ordenador.

Con el incremento de los ataques en Internet, la necesidad de protección se convierte en algo evidente.

Soluciones

Una cuestión de elección

La seguridad y los programas de protección han existido desde que los ordenadores se convirtieron, por primera vez, en objetivos para personas malintencionadas, virus y otras amenazas.

Desafortunadamente, con tanta variedad de ataques, no existe una solución integral para proteger su ordenador personal.

La mayoría de los usuarios no sabe muy bien cómo protegerse.

Antes de la gran popularización actual de Internet, el único programa que los usuarios tenían que instalar era un antivirus.

Hoy en día un buen antivirus es sólo un componente de un escudo de seguridad, que cada usuario debe construir.

Dada la gran cantidad de ataques e intrusiones a los sistemas, un cortafuegos personal se convierte en **imprescindible** para todos los usuarios conectados a Internet.

Cortafuegos

Un cortafuegos es una barrera entre su ordenador e Internet.

Controla todo el tráfico de datos desde y hacia su ordenador, bloquea los datos maliciosos y permite recibir únicamente el tráfico legítimo.

Existen dos tipos de cortafuegos: los basados en equipamiento físico (*hardware*) y los programas (*software*) que cumplen tal función.

Los cortafuegos basados en equipamiento físico son muy costosos, y generalmente los utilizan las corporaciones para proteger sus redes locales.

Aún a pesar de su alto precio, las técnicas utilizadas por los cortafuegos de *hardware* pueden dejar espacios para los agresores.

El cortafuegos personal se basa en una aplicación instalada en su ordenador para protegerla contra cualquier amenaza externa o incluso interna.

El programa puede hacerse mucho más inteligente que el *hardware*, puede actualizarse fácilmente y es más económico.

Un cortafuegos personal puede proteger su ordenador contra los ataques de agresores informáticos o códigos maliciosos, como los troyanos, programas espía y otras amenazas similares, incluyendo los anuncios publicitarios molestos.

Outpost Firewall Pro

Outpost Firewall Pro puede brindarle seguridad, privacidad, control y facilidad de uso.

Outpost es, de acuerdo con muchos laboratorios de pruebas independientes, la mejor solución integrada para proteger su ordenador. De hecho, le brinda protección contra cualquier posible amenaza en el tráfico de Internet.

Outpost fue diseñado para el usuario promedio, no sólo para los expertos en informática. Por lo tanto, no requiere prácticamente de ninguna capacitación para utilizarlo.

A continuación, se brinda una idea de cómo muchos ordenadores hogareños se están beneficiando con el cortafuegos personal de Outpost.

Seguridad y privacidad

Con Outpost, los usuarios hogareños tienen protegido su ordenador contra todos los posibles ataques desde Internet, incluyendo cualquier contenido malicioso existente en las páginas que navegan.

Outpost también ofrece protección para sus datos confidenciales, de forma tal que no tendrá que instalar ningún programa adicional para proteger su privacidad cuando navega.

Control de acceso a sitios indeseados

Los niños a menudo utilizan los ordenadores antes de aprender a escribir.

Para los padres, es a veces alarmante imaginar el tipo de sitios de Internet que sus hijos podrían llegar a ver.

Outpost le permite evitar el acceso a todos los sitios indeseables.

Outpost Personal Firewall puede proteger a sus hijos de los sitios ilegales y/o inapropiados en Internet.

Puede crear una lista de sitios de Internet prohibidos, o incluso bloquear ciertos sitios que contengan ciertas palabras típicas, como **sexo**, **bombas**, entre otras.

Fácil de usar

A diferencia de la mayoría de los cortafuegos de uso personal, Outpost fue desarrollado para ser utilizado eficientemente por todos los usuarios, incluso aquellos que carecen de experiencia.

La protección comienza en el momento de instalarlo.

Outpost luce y funciona como el Explorador de Windows, por lo cual la forma de utilizarlo es muy sencilla e intuitiva.

Actualizaciones automáticas

Con la función de actualización automática de Outpost, los usuarios no tienen que visitar nuestro sitio de Internet cada vez que deseen verificar si existe alguna actualización disponible.

Outpost actualiza y mejora continuamente sus funciones, para protegerlo contra todas las nuevas amenazas.

Arquitectura abierta y complementos

Además de las características mencionadas, Agnitum Outpost es el primer cortafuegos personal de arquitectura abierta, que acepta complementos de terceras partes.

Esta característica lo pone un paso adelante en comparación con otros cortafuegos.

Un complemento es un módulo independiente que puede insertarse en un programa para ampliar sus capacidades.

Con esta tecnología, los desarrolladores de terceras partes pueden mejorar fácilmente la funcionalidad de Outpost, al crear y distribuir sus propios complementos, usando las especificaciones de arquitectura abierta de Outpost.

Con Outpost, usted obtiene una solución integrada para sus necesidades de seguridad.

Outpost combina su premiada tecnología inteligente, con una extraordinaria facilidad de uso.

Los creadores de programas nocivos no esperan a que usted obtenga las herramientas que necesita para su protección.

¡Comience a proteger su ordenador ahora mismo, instalando Outpost!

Invierta algunos minutos y ahórrese horas de problemas.

¡Outpost es la solución inteligente!