Dr.WEB®
desde 1992

¡Configura Dr.Web contra cifradores!

Recomendaciones para minimizar el riesgo de infección por un troyano extorsionista

Los troyanos cifradores (familia Trojan.Encoder) – son programas nocivos que buscan en las unidades del equipo infectado o en la memoria del dispositivo móvil los archivos de usuario, luego los cifran y demandan a la víctima un rescate por descifrarlos.

Todos los cifradores son archivos nocivos (troyanos) que **no pueden difundirse ni ser iniciados automáticamente**. Según las estadísticas de Doctor Web

En más de 90% de los casos	Sólo en un 10% de los casos
los usuarios mismos inician cifradores en su equipo.	es posible descifrar.

Es importante saberlo

Los grupos criminales que se dedican al desarrollo de programas nocivos, hacen pruebas para que los mismos no **sean detectados** por todas las soluciones antivirus actuales. Como resultado, se lanzan solo los programas nocivos que nunca pueden ser detectados por antivirus (antes de recibir actualizaciones).

Un cifrador puede penetrar hasta en un equipo protegido por cualquier antivirus – si el troyano aún es desconocido para la base de virus o si el antivirus no contiene tecnologías de protección preventiva. Ningún antivirus detecta todos los programas nocivos en cualquier momento.

Es decir, cada uno puede ser infectado por un cifrador nuevo y desconocido si Vd. no ha configurado su sistema de protección

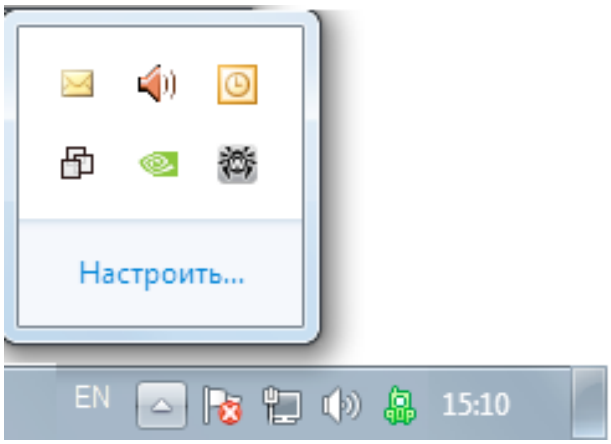
Configura Dr.Web

Las reglas básicas de configuración de Dr.Web ayudan a prevenir una infección por un cifrador — hasta un desconocido para el núcleo antivirus.

Dr.Web debe siempre estar activado

Y si su equipo está conectado a Internet o tiene un dispositivo externo de información conectado aún no escaneado en busca de virus antes de conectarse, - nunca debe desactivar Dr.Web en este momento.

Si Dr.Web está activado y, por lo tanto, protege su PC, lo confirma este icono del agente Dr.Web en la bandeja del sistema.



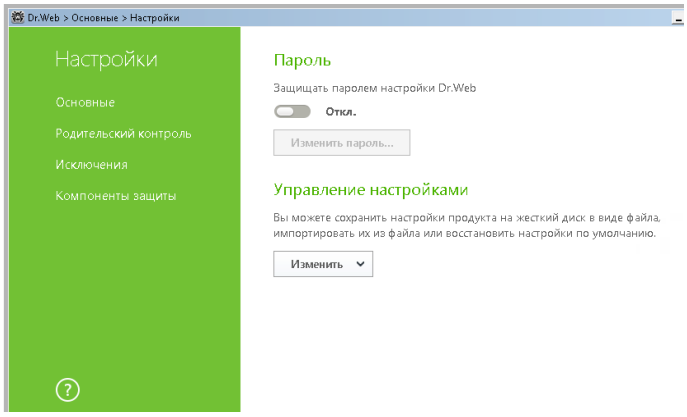
Si no hay icono del agente, un icono con un signo de exclamación o una cruz quiere decir que Dr.Web está desactivado y el equipo no tiene protección antivirus. En este caso, reinicie el equipo. Si el problema persiste — enseguida contacte con el servicio de soporte Doctor Web.

¿Su Dr.Web está activado ahora?

Debe establecer la contraseña de Dr.Web

En caso de establecer la contraseña, no será posible desactivar la protección Dr.Web — hasta en caso de un hackeo.

Para establecer la contraseña de acceso a Dr.Web



Haga clic sobre (que se cambiará por) y, al hacer clic sobre el icono que aparece , seleccione **General** en el menú **Configuración**. Haga clic sobre el conmutador y luego sobre **Cambiar contraseña**.

¡Atención! *No se recomiende establecer la contraseña que coincide con la contraseña de acceso al equipo o dispositivo. No se puede guardar la contraseña de Dr.Web en el mismo equipo.*

¿Su Dr.Web tiene establecida la contraseña?

Todos los componentes de protección Dr.Web siempre deben estar activados

Cada componente Dr.Web Security Space participa en la protección contra troyanos extorsionistas.

La desactivación — hasta de un solo componente y temporalmente — significa reducción de protección considerable.

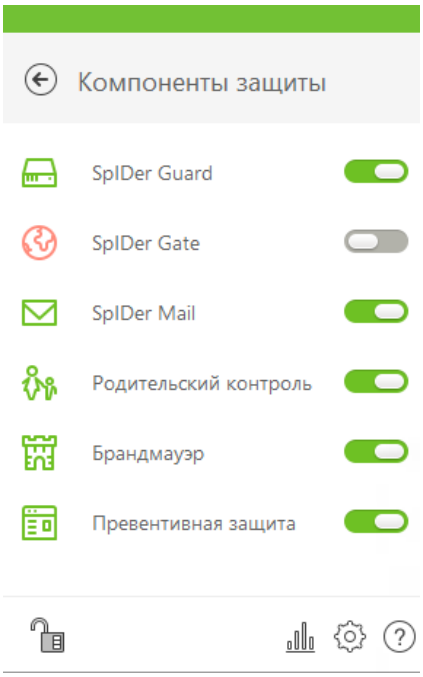
- **Dr.Web SpIDer Guard** detectará los programas nocivos en el momento de inicio de los mismos — hasta en caso de haber recibido los componentes nocivos cifrados y no detectarlos en el momento de descarga.

- Así mismo, un cifrador puede penetrar en un equipo a través de un mensaje de correo electrónico. Normalmente, este mensaje suele contener un adjunto nocivo o un enlace creado a propósito. **El Antispam** Dr.Web bloquea los mensajes de contenido nocivo característico para los mensajes de malintencionados — hasta si el núcleo antivirus aún no ha recibido la actualización que contiene la información sobre la amenaza más nueva.
  El Antispam Dr.Web no necesita formación — él mismo sabe cómo actuar.
- **Dr.Web SpIDer Gate** y **el Control Parental** no le permitirán ir al sitio web peligroso en caso de recibir un enlace para descargar en un mensaje. El servicio de escaneo del tráfico de correo y web que forma parte de Dr.Web Security Space se basa en algoritmos únicos que aseguran la máxima velocidad de escaneo y la calidad óptima de detección de programas nocivos.
- El Firewall Dr.Web permite configurar las restricciones para programas que tienen acceso a Interne.

Y estos son solo algunos componentes Dr.Web que aseguran la detección de virus y troyanos.

Para averiguar si su Dr.Web tiene componentes desconectados

Consulte la bandeja del sistema — si su Dr.Web tiene componentes desactivados, el icono Dr.Web tendrб aspecto siguiente:



Para ver qué componentes están desactivados

Haga clic sobre el icono del agente Dr.Web y luego sobre **Componentes de protección** — se abrirá el menú del agente Dr.Web.

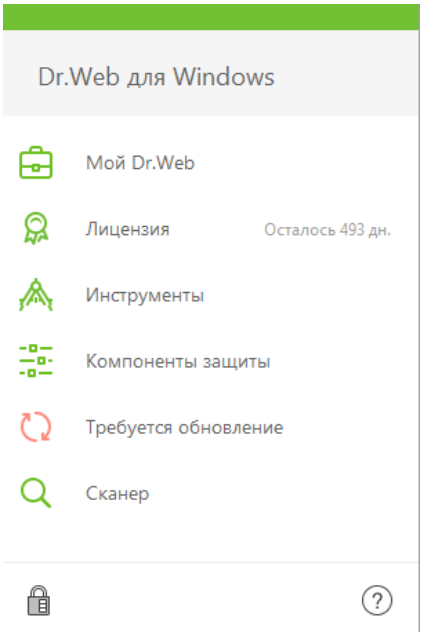
¿Su Dr.Web tiene todos los componentes activados?

El antivirus debe ser actualizado a menudo

El antivirus debe ser actualizado una vez recibidas las actualizaciones.
Para realizarlo, basta con no desactivar la configuración de las actualizaciones establecida por el desarrollador de Dr.Web, — el antivirus se actualizará automáticamente y de forma oportuna.

Pero también es muy importante REINICIAR EL PC una vez recibidas las actualizaciones que requieren este reinicio, — siempre que Dr.Web lo solicite. Porque solo una vez reiniciado, se instalan los nuevos controladores de intercepción de programas nocivos anteriormente desconocidos y corrección de las vulnerabilidades potenciales de protección Dr.Web.

¡Atención! *Cada día hasta un millón de nuevos archivos potencialmente peligrosos llegan al laboratorio antivirus Doctor Web. En caso de no actualizar Dr.Web hasta durante unas horas se puede omitir centenares archivos nocivos anteriormente desconocidos (así mismo, para el analizador heurístico Dr.Web). Un solo troyano banker necesita de 1 a 3 minutos para robar dinero desde la cuenta del usuario.*



Para comprobar la fecha y la actualidad de actualizaciones

Haga clic sobre en la bandeja del sistema. El estado de actualizaciones se visualizará en la bandeja del sistema.

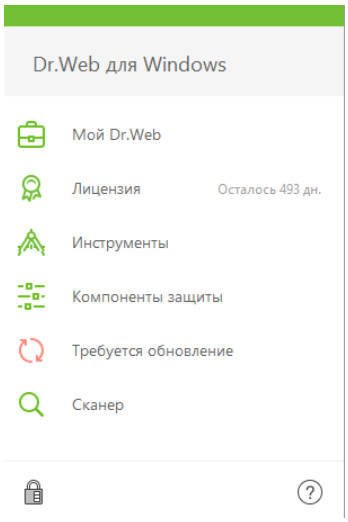
¿Cuándo se instaló la última actualización en su Dr.Web?

Las excepciones de escaneo solo pueden usarse en casos de emergencia

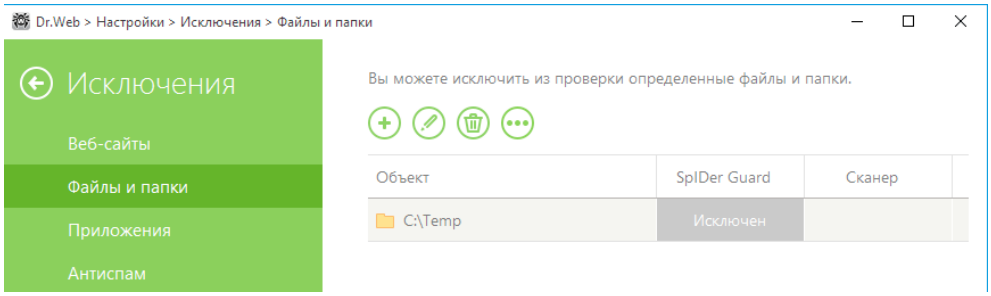
Las excepciones del escaneo pueden acelerar el escaneo, pero normalmente al reducir el nivel de seguridad. Los creadores de virus saben QUÉ EXACTAMENTE los usuarios suelen excluir del escaneo y lo usan activamente para sus delincuencias.

Nuestros programas están optimizados al máximo y ahorran los recursos del equipo. No recomendamos excluir nada del escaneo Dr.Web sin consultarnos, porque no cada usuario tiene bastantes conocimientos para valorar los riesgos de esta configuración. Las excepciones son un modo de esquivar alguna situación problemática. Solo el soporte técnico de Doctor Web puede recomendar cómo hacerlo bien.

Para comprobar si en su Dr.Web se usan las excepciones del escaneo que reducen el nivel de protección



Haga clic sobre en la bandeja del sistema. En el menú que aparece haga clic sobre (el icono se cambiará por) y, al hacer clic sobre el icono que aparece , seleccione **Configuración → Excepciones**.



¡Atención! *Si las excepciones tienen establecidas las máscaras de tipo *.exe o *.dll, Dr.Web no escaneará todos los objetos que corresponden a esta máscara, — es decir, todos los archivos ejecutables y bibliotecas de software.*

¡Atención! *No se recomienda excluir el escaneo del tráfico para programas usados porque esto puede impedir el escaneo de software descargado por estos programas.*

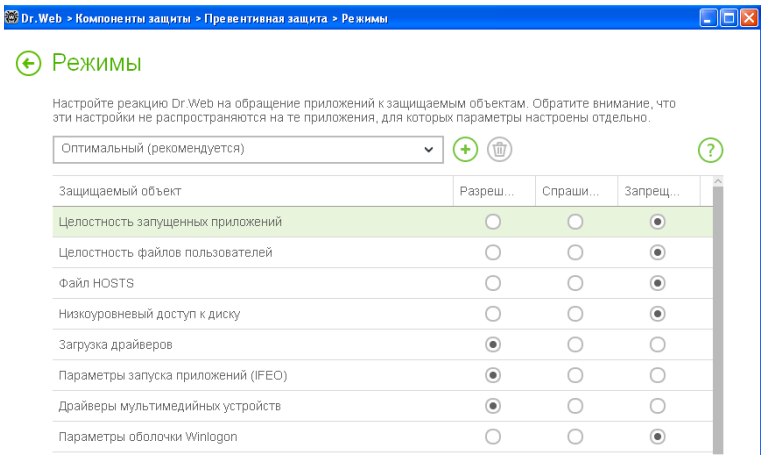
¿Su Dr.Web tiene establecida alguna excepción del escaneo?

La protección preventiva debe estar habilitada

Hoy en día la Protección preventiva es uno de los componentes más importantes en el sistema de protección integral Dr.Web.

Al detectar comportamiento de un programa sospechoso (aún desconocido para Dr.Web) similar a los modelos conocidos de comportamiento de programas nocivos ya conocidos, la Protección preventiva Dr.Web sabe detectar y bloquear estos programas gracias a un conjunto de tecnologías que funcionan adelantando y no dependen de firmas en la base de virus Dr.Web.

No se recomienda desactivar la protección preventiva — su funcionamiento prácticamente previene la posibilidad de robar sus datos y dinero para troyanos cifradores, bloqueadores, troyanos bancarios y otros programas nocivos peligrosos.



¡IMPORTANTE! *Para la protección extra contra cifradores, en la configuración del componente "Protección preventiva" siempre debe establecer «Permitir» para la «Integridad de aplicaciones activadas» y la «Integridad de archivos de usuarios».*

¿Y su Dr.Web tiene habilitada esta configuración?

Si el PC está conectado a Internet, la Protección preventiva recibe la información sobre los algoritmos más actuales desde el servicio en línea en la nube Dr.Web Cloud para afrontar las amenazas desconocidas. Esto proporciona la protección contra los programas nocivos recibidos por los analistas Dr.Web ya una vez realizadas las últimas actualizaciones del antivirus en su equipo. Normalmente las actualizaciones tradicionales llegan al equipo no más de una vez cada hora.

Y en Dr.Web Cloud la información siempre está actualizada porque se añade al mismo enseguida al enterarse los analistas Dr.Web de la misma. El uso de la base de conocimiento de la nube mejora bastante la protección contra amenazas que usan las vulnerabilidades de “hora cero”.

¿Su Dr.Web tiene habilitada la Nube Dr.Web?

De forma predeterminada, se establece el nivel Óptimo de la Protección preventiva Dr.Web. Para más información sobre la configuración de la Protección preventiva Dr.Web, véase aquí.

La protección preventiva tiene un sistema de perfiles que pueden ser usados para crear reglas flexibles para aplicaciones de confianza y así mismo prevenir conflictos de funcionamiento de la Protección preventiva Dr.Web. Para más información sobre la configuración de perfiles de la Protección preventiva Dr.Web, consulte la documentación.

La protección contra la pérdida de datos debe estar habilitada y configurada

«La Protección contra la pérdida de datos» permite almacenar los archivos más importantes del usuario en un almacén especial protegido por Dr.Web.

A diferencia de programas ordinarios de la copia de seguridad, Dr.Web crea y protege contra el acceso no sancionado de los malintencionados el almacén con las copias de archivos. Hasta si un troyano más nuevo (aún desconocido para Dr.Web) penetra en su PC, el uso de la «Protección contra la pérdida de datos» salvará sus archivos. Y si aún así un troyano logra cifrar sus archivos, Vd. puede recuperarlos sin ayuda, sin contactar con el servicio de soporte técnico Doctor Web.

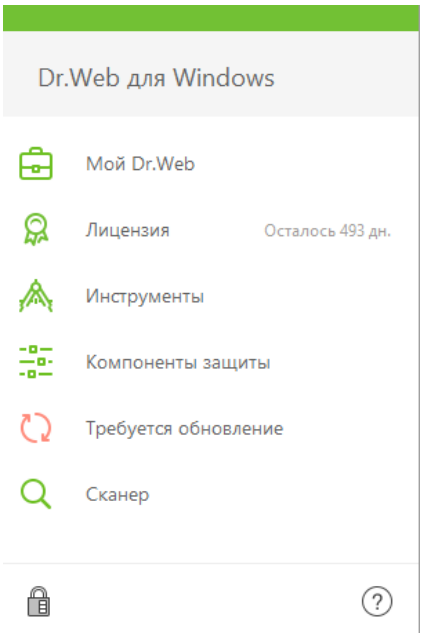
De forma predeterminada, este componente no está activado, porque para su funcionamiento hay que indicar los datos que deben ser guardados y configurar el sitio y el modo de almacenamiento de los datos.

¿Y su Dr.Web tiene habilitada y configurada «la Protección contra la pérdida de datos»?

La licencia Dr.Web debe ser actual

Para que Dr.Web proteja su PC, la licencia debe ser activa (válida).

Una vez expirada la licencia, todos los componentes de protección Dr.Web dejan de funcionar.



Para averiguar el periodo de validez de su licencia Dr.Web

Haga clic sobre en la bandeja del sistema. Si la licencia es válida, en el menú que se abre se visualizará el número de días que se quedan hasta la expiración de la licencia.

Así mismo, se puede averiguar el periodo de validez de la licencia Dr.Web en el Administrador de licencias del sitio web.

¿Y su Dr.Web tiene licencia activa ahora?

Qué hacer en caso de una infección por un cifrador

Para que los expertos de Doctor Web puedan recuperar los archivos cifrados,
NO SE PUEDE:

- cambiar la extensión de los archivos cifrados;
- reinstalar el sistema operativo;
- usar algún programa para descifrar/recuperar los datos sin ayuda;
- borrar/ cambiar nombre de archivos y programas (así mismo, los temporales);
- realizar acciones irrecuperables para desinfectar/borrar objetos nocivos.

Como resultado de estas acciones, Vd. puede perder sus datos para siempre — hasta una utilidad de descifrado especial no podrá localizarlos ni recuperarlos.

Por eso es mejor no realizar ninguna acción en el equipo infectado hasta recibir una respuesta de Doctor Web sobre la posibilidad de recuperar archivos.

Reglas de comportamiento en caso de infección por un troyano extorsionista	Plantillas de denuncias a policía

Recuperación gratuita de archivos cifrados por un troyano extorsionista

se ofrece para titulares de licencias comerciales válidas Dr.Web Security Space, Dr.Web Enterprise Security Suite (Protección integral) y abonados al servicio «el Antivirus Dr.Web» (paquete de tarifas Dr.Web Premium) — en caso de cumplir con estos requisitos en el momento del incidente.

Para los usuarios de otros antivirus este servicio es de pago — habrá que adquirir la licencia de Dr.Web Rescue Pack.

Contenido de la licencia

- Utilidad de descifrado
- Licencia Dr.Web Security Space para 1 PC por 2 años

Solicitud para descifrar

El conocimiento es un arma poderosa contra los troyanos cifradores

Sobre cómo configurar correctamente el sistema de protección contra los troyanos extorsionistas, informa el curso de formación **DWCERT-070-6 «Protección de las estaciones de trabajo y servidores de archivos Windows contra los programas cifradores»**, disponible en el siguiente enlace https://training.drweb.ru/users.

¿Todos engañan? ¡Pero tenemos “El mundo de antivirus”!

En las páginas del proyecto formativo “El mundo de antivirus”, en el tema “Cifrarlo todo”, informamos sobre cómo afrontar a los troyanos cifradores.

Todas las ediciones del tema «Cifrarlo todo»

Reglas de la higiene

Los cifradores se difunden ampliamente por correo — supuestamente, en nombre de la inspección fiscal, el juzgado o su gente conocida, como si fuera un CV, documentos de contabilidad, etc. En caso de haber recibido un mensaje sospechoso con un adjunto omitido por Dr.Web, el mismo puede contener un cifrador aún desconocido para el antivirus.

Envíe este adjunto para el análisis al laboratorio antivirus de Doctor Web https://vms.drweb.ru/sendvirus y espera la respuesta de un experto.

Así Vd. ayudará no solo a si mismo, al prevenir el cifrado de los datos, sino también a miles de víctimas potenciales de ciberdelincuentes.

Vd. puede ayudar a afrontar a ciberdelincuentes

El cifrado de datos es una amenaza importante, y los archivos dañados es un problema serio. Pero se puede afrontarlo, y hay que hacerlo. Le rogamos a Vd. como víctima presentar una denuncia a la policía sobre el acceso no sancionado a su equipo, la difusión de programas nocivos y extorsión.

Dr.WEB®
desde 1992

Sobre la empresa Doctor Web

Doctor Web es un productor ruso de los medios antivirus de protección de la información bajo la marca Dr.Web. Los productos Dr. Web se desarrollan a partir del año 1992. Es una empresa clave en el mercado ruso del software para asegurar la necesidad básica del negocio - la seguridad de información.

Doctor Web es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas malintencionados. La empresa tiene su propio laboratorio antivirus, un servicio global de supervisión de virus y un servicio de soporte técnico.

El objetivo estratégico de la empresa, clave para todo el personal, es la creación de los mejores medios de protección antivirus que cumplen con todos los requisitos modernos para este tipo de programas, así como el desarrollo de las mejores soluciones tecnológicas que permiten a los usuarios afrontar con éxito cualquier tipo de amenaza informática.

Formación
Área de formación en línea Dr.Web (debe registrarse)
Cursos para ingenieros | Cursos para usuarios | Folletos

Materiales de formación
El mundo de antivirus | WebIQmetr | Folletos

Oficina central de Doctor Web S.L.
125040, Rusia, Moscú, c/3 Yamskogo Polya, 2, edif.12A

Teléfonos

Cómo llegar

Contactos para prensa

Oficinas fuera de Rusia

www.drweb.com | free.drweb.com | www.av-desk.com | curenet.drweb.com

Síganos en las en las redes sociales