Dr.WEB®
since 1992

Configure Dr.Web to protect your computer from encryption ransomware!

Recommendations on how to lower your computer's risk of getting infected by encryption ransomware

Encryption ransomware (Trojan.Encoder) programs are malicious programs that search for user data on the disks of infected desktops or in the memory of compromised mobile devices, encrypt it, and demand a ransom for its decryption.

Encryption ransomware **cannot replicate itself or launch itself independently**. According to Doctor Web statistics

Users are to blame for **over 90%** of	**Only 10%** of
encryption ransomware incidents.	encrypted files can be decrypted.

Worth knowing

Cybercrime gangs involved in developing malicious programs test them against all current anti-virus solutions to make sure that their malware can bypass anti-virus security. As a result, only malicious programs that aren't detected by anti-viruses (because they have not yet acquired the corresponding virus definitions) are released into the wild.

Encryption ransomware can penetrate any computer, even one protected by an anti-virus if the Trojan involved hasn't yet been added to the virus database or if the anti-virus does not incorporate proactive protection technologies. No anti-virus can, at any point in time, detect all malicious programs.

This means that any system, including yours, can be infected by new, unknown ransomware — if you have not configured your protection system

Configure Dr.Web

Simple configuration rules help avoid ransomware infections–even those caused by programs that are unknown to the anti-virus engine.

Always keep your Dr.Web anti-virus enabled

And if your PC is connected to the Internet or you are using removable media that hasn't been scanned for viruses—it is strongly recommended that you do not disable the Dr.Web anti-virus.

The below Dr.Web Agent icon in the system tray indicates that Dr.Web is enabled and thus protecting your PC.

If the Agent icon is missing or you see an icon with an exclamation mark or cross, the Dr.Web anti-virus is disabled and your PC is unprotected. In this case, urgently restart your PC. If the problem persists, immediately contact the Doctor Web support service.

Is your Dr.Web enabled right now?

Password-protect your Dr.Web

A password ensures that your Dr.Web protection won't be disabled—even if your PC gets hacked.

To set a password to access Dr.Web

Click on the icon (its appearance will change to). Press the icon, and in the **Settings** menu, select **Main**. Toggle on the corresponding option, and click on **Change password**.

Important! *Using a password that matches your user account on a computer or device is not recommended.*

Is your Dr.Web password-protected?

All the Dr.Web protection components must always be enabled

Each component of Dr.Web Security Space plays a role in fending off encryption ransomware.

Disabling—just one of them, even only temporarily—will inevitably reduce the level of protection.

- **Dr.Web SpIDer Guard** detects malicious programs as soon as they launch even if it receives the malicious components in an encrypted format and did not detect them at the moment of penetration
- Encryption ransomware can penetrate a system even via an email message. As a rule, it can be attached to a message or downloaded via a link. Dr.Web **Anti-spam** filters out emails containing malicious content that has all the characteristic hallmarks of cybercriminals—even if the anti-virus engine is not yet updated with information about this latest threat.
  You don't need to train it—it knows what to do!

- **Dr.Web SpIDer Gate** and **Parental Control** will not allow you to visit a dangerous site even if you receive a link to download a Trojan in an email message. Dr.Web Security Space includes an email- and web-traffic scanning service based on unique algorithms that ensure the highest possible scanning speed and high-quality malware detection.
- Dr.Web Firewall lets you configure restrictions for programs that can connect to the Internet.

And that's not the complete list of Dr.Web components capable of detecting viruses and Trojans!

To find out whether any of your Dr.Web components are disabled

Check the system tray—if any Dr.Web component is disabled, the icon will look like this:

To see what components are disabled

Click on the Dr.Web Agent's icon, and select **Protection components**—the Dr.Web Agent menu will open.

Are all of your Dr.Web components enabled?

Update your anti-virus regularly

Update your anti-virus immediately as soon as updates are released. do this, it is enough to disable the update settings specified by the Dr.Web developer— the anti-virus will update itself in a timely manner.

In addition, it is important to REBOOT your PC after updates that require such action— no matter how often Dr.Web prompts you to do that. This is important because only after a system reboot are new interception hooks installed and potential Dr.Web security vulnerabilities patched.

Attention! *In just one day the Doctor Web virus laboratory receives up to a million new, potentially malicious files. If Dr.Web is not updated within even several hours, hundreds of previously unknown (including to the Dr.Web heuristic analyser) malicious files can be skipped over. Meanwhile, a single banking Trojan needs just one to three minutes to steal money from a user's bank account.*

To check the date and relevancy of updates

Click on the icon in the system tray. The status of updates will be displayed in the newly appeared menu.

When did you last update your Dr.Web?

Use scan exclusions in case of emergency only

Exclusions can accelerate scanning but often at the cost of lowering the security level. Virus writers know THAT users like to use this option, and actively use it for their criminal purposes.

Our programs are optimised and consume system resources carefully. We do not recommend that you exclude any website from Dr.Web scanning because not every user has enough knowledge to assess the risks of such a configuration. Exclusions are a way of bypassing any problematic situations. And only the Doctor Web support service can advise you how to do this properly.

To check whether any scan exclusions are lowering your security level

Click on the icon in the system tray. In the newly appeared window, click on the icon (its appearance will change to). Press the icon, and in the **Settings** menu, select **Exclusions**.

Important! *If a mask, such as *.exe or *.dll, is added to the list of exclusions, Dr.Web will not check all the objects that have that mask—i.e., all executable files and program libraries!*

Important! *You should not exclude programs you use from traffic scanning—if you do, Dr.Web won't scan any malicious software downloaded by those programs.*

Have any scan exclusions been added to your Dr.Web?

Enable the Preventive Protection component

Today, Preventive Protection is one of the most important components in the Dr.Web comprehensive protection system.

Dr.Web Preventive Protection can recognise suspicious (currently unknown to Dr.Web) programs that have similar behaviour patterns and block their operation. This is because none of the software's proactive technologies depend on the signatures of these suspicious programs being present in the Dr.Web virus database.

Disabling Preventive Protection is not recommended because this component significantly impedes the ability of the following to steal your data and money: encryption ransomware, ransomware lockers, banking Trojans, and other types of the most dangerous malware.

Important! *To fortify your protection against encryption ransomware, in the Preventive Protection settings, "Block" must always be set for "Integrity of running applications" and "Integrity of user files".*

Is this option enabled in your Dr.Web?

If your PC is connected to the Internet, the Preventive Protection component receives data from Dr.Web Cloud on the algorithms most relevant for neutralising unknown threats. This ensures that your computer is protected against malware that was detected by Doctor Web's analysts after the anti-virus on your computer was last updated. Usually, traditional updates get onto a computer no more frequently than once per hour. Dr.Web Cloud always contains fresh information because it is updated constantly by Doctor Web's virus analysts. Using the cloud knowledge base makes a computer significantly more secure against threats that use zero-hour vulnerabilities.

Is Dr.Web Cloud enabled in your Dr.Web?

The **Optimal** mode in Dr.Web Preventive Protection is enabled by default. Learn more about the Dr.Web Preventive Protection settings here.

Preventive Protection has its own system of profiles that can be used to create flexible rules for applications in order to prevent conflicts that may otherwise be caused by the Dr.Web Preventive Protection component. Learn more about configuring Dr.Web Preventive Protection profiles in the documentation.

Is the Preventive Protection component enabled in your Dr.Web?

Data Loss Prevention must be enabled and configured

The Data Loss Prevention component saves a user's most important files in a special protected Dr.Web storage.

Unlike conventional back-up programs, Dr.Web creates backups and protects them from intruders. Even if the latest Trojan (one not yet known to Dr.Web) penetrates your PC, the Data Loss Prevention component will save your files. And even if a Trojan does encrypt your files, you will be able to restore them without Doctor Web's assistance.

This component is disabled by default because you need to specify what data needs to be saved and configure where and how you want to store your data.

Is the Data Loss Prevention component enabled and configured in your Dr.Web?

Your Dr.Web license must be valid

Your license must be active in order for the Dr.Web anti-virus to protect your PC.

Once your license expires, all the protection components of Dr.Web will be unavailable.

To find out whether your Dr.Web license is valid

Click on the icon in the system tray. If your license is valid, you will see, in the newly appeared menu, the number of days remaining on the license.

The validity period of your Dr.Web license can also be viewed in the License Manager on the Doctor Web site.

Is your Dr.Web license valid?

What to do if your system gets infected by encryption ransomware

For Doctor Web's specialists to be able to recover your corrupted files successfully, you MUST NOT:

- change the file name extensions of the encrypted files;
- reinstall the operating system;
- use some program to decrypt/recover the data;
- delete/rename any files (including temporary ones) and applications;
- take any irreversible actions such as curing/removing the malware.

Doing any of the above could result in data loss so permanent that even a special decryption utility won't be able to find the files and restore them.

That's why you should not do anything with your infected computer until you receive a reply from Doctor Web's support service about recovering your files.

Rules of conduct when a system gets infected by encryption ransomware	Sample police statements

Free recovery of files corrupted by encryption ransomware

is available to owners of valid commercial licenses for Dr.Web Security Space and Dr.Web Enterprise Security Suite (Comprehensive protection) and for Dr.Web Anti-virus Service subscribers (Dr.Web Premium package)—provided these requirements were met at the moment the incident occurred.

The service is provided on a paid basis to users of other anti-viruses—such individuals must purchase a license for Dr.Web Rescue Pack.

The license covers:

- Decryption utility
- Dr.Web Security Space license for 1 PC for 2 years

File a decryption request

Knowledge is a powerful weapon against encryption ransomware

Learn how to protect your system against ransomware in the training course **DWCERT-070-6 "Protection from encryption ransomware for Windows PCs and file servers"**, which you can download here https://training.drweb.com/users.

Are you surrounded by misinformation? Thankfully, you have the Anti-virus Times!

The pages of our Anti-virus Times educational project, specifically articles in the category "Encrypt everything", will tell you how to protect your system against ransomware.

All issues in the category "Encrypt everything"

New issues on various aspects of IT security are published every banking day—join our Anti-virus Times readers, and tell all of your family members, friends, and colleagues about the project! All project publications

The rules of “basic hygiene”

Encryption ransomware spreads in bulk via emails that are ostensibly from tax authorities, courts of law, and even friends. Attachments containing malware are made to look like CVs, accounting documents, etc. If you’ve received a suspicious email with an attachment, and Dr.Web didn’t react to it, the attachment may contain encryption ransomware that the anti-virus doesn’t yet recognise.

Send the attachment for analysis to the Doctor Web anti-virus laboratory at https://vms.drweb.com/sendvirus, and wait for a reply.

By doing so, you will not only keep your files safe but also help thousands of potential cybercrime victims.

You can help stop cybercriminals

Encryption ransomware is a severe threat, and corrupted files can be a serious problem. But we can and must fight it. We urge you, as a victim, to go to your nearest police precinct and file a complaint that unauthorized access was gained to your computer, malware was distributed, and extortion was involved. You can find sample police statements on our website: http://legal.drweb.com/templates.

Dr.WEB®
since 1992

About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web products have been in development since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business — information security.

Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. The company has its own anti-virus laboratory, a global virus-monitoring service, and a technical support service.

Doctor Web's strategic goal upon which the efforts of its entire staff are focused is to create superlative anti-virus software that meets all the current demands of this market segment, and to develop new technologies that allow users to be fully armed against all types of computer threats.

Training
My Dr.Web Training Portal (registration required)
Courses for engineers | Courses for users | Brochures

Education
The Anti-virus Times | WebIQmetr | Brochures

Contacts
Headquarters Doctor Web Ltd.
125040, Russia, Moscow, 3rd street Yamskogo polya 2-12A

Phone numbers

How to reach us

Media contacts

Doctor Web Offices outside the Russian Federation

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

Join us on social networking sites