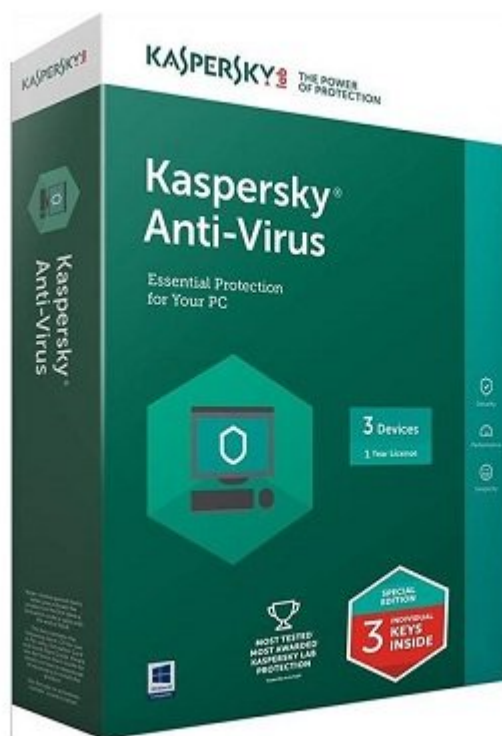


□□□□□□□□ □□□□□□ □□□□ □□

[illegible][illegible]

00000 0 000000000 00 0000 00000 0000 0000 0000000000 0 000000 00000 00 00000000 0000000000 000 00000
 00000000 0000000000 0000 00 0000000000 .0000 00000000 00000 0000000000 00 0000000 00 00000000 00000000 0000000000
 0000000000 0000000000 00 00000 000000 00 000000 00000 00000 00000 00000 0000 0000 000000 0000000000 0000 00
 00000 00 .00000 00000 000000 00 000000 00000 00 000 0000000 000000 00 000 0000000 00000 00000000
 .00000 000000 0000 00 00 000000000 000000000 0000 0000000000 00 00000 0000000 000 00000

20

7.1. .

... 67 98 95.

Kaspersky Secure Connection VPN Kaspersky Total Security 200.

System Watcher

Protection Settings (2).

1. **Rescue Mode** (3 steps). This mode is used to scan and remove malware from a computer that is infected. It is a safe mode that allows you to scan and remove malware without the risk of the malware interfering with the scan.

2. **Rescue Disk** (3 steps). This is a bootable disk that you can use to scan and remove malware from a computer that is infected. It is a safe mode that allows you to scan and remove malware without the risk of the malware interfering with the scan.

3. **Privacy Cleaner** (3 steps). This tool is used to clean up your system and remove any traces of malware. It will scan your system for any files or folders that may contain malware and remove them.

4. **Browser Configuration** (3 steps). This tool is used to configure your web browser to prevent malware from being downloaded or installed. It will scan your browser for any settings that may be vulnerable to malware and configure them to be secure.

5. **System Restore** (3 steps). This tool is used to restore your system to a previous state, before the malware was installed. It will scan your system for any files or folders that may contain malware and remove them.

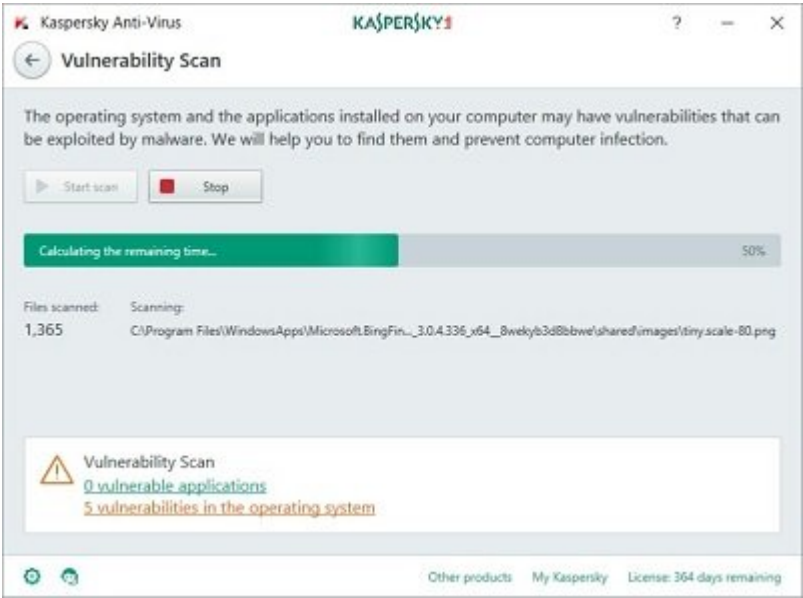
6. **Antivirus Scan** (3 steps). This tool is used to scan your system for any malware that may be present. It will scan your system for any files or folders that may contain malware and remove them.

7. **Malware Removal Tool** (3 steps). This tool is used to remove any malware that may be present on your system. It will scan your system for any files or folders that may contain malware and remove them.

8. **System Update** (3 steps). This tool is used to update your system with the latest security patches. It will scan your system for any updates that are available and install them.

9. **System Backup** (3 steps). This tool is used to create a backup of your system. It will scan your system for any files or folders that may contain malware and remove them.

10. **System Restore** (3 steps). This tool is used to restore your system to a previous state, before the malware was installed. It will scan your system for any files or folders that may contain malware and remove them.



1. **System Restore** (3 steps). This tool is used to restore your system to a previous state, before the malware was installed. It will scan your system for any files or folders that may contain malware and remove them.

2. **System Backup** (3 steps). This tool is used to create a backup of your system. It will scan your system for any files or folders that may contain malware and remove them.

3. **System Update** (3 steps). This tool is used to update your system with the latest security patches. It will scan your system for any updates that are available and install them.

4. **Malware Removal Tool** (3 steps). This tool is used to remove any malware that may be present on your system. It will scan your system for any files or folders that may contain malware and remove them.

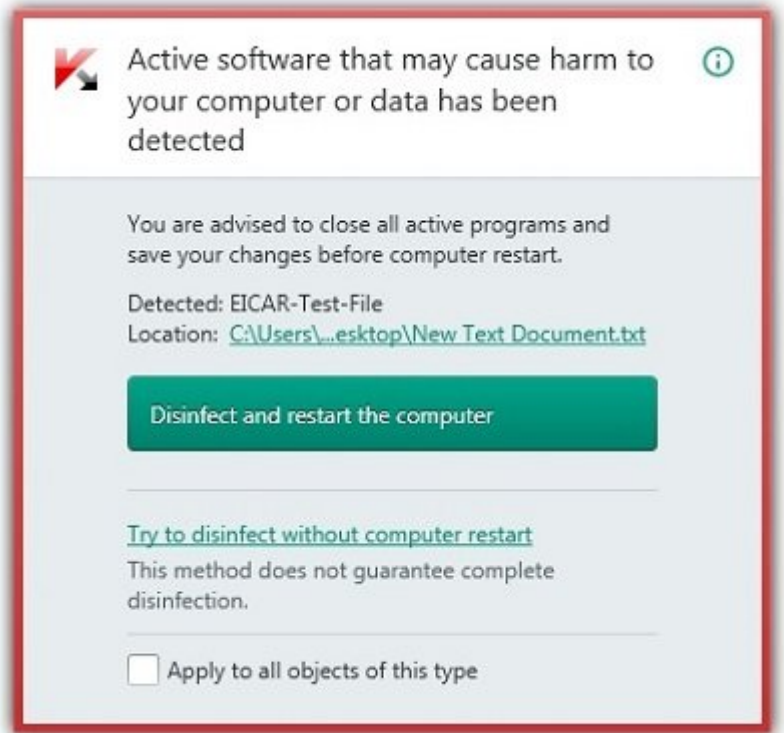
5. **Antivirus Scan** (3 steps). This tool is used to scan your system for any malware that may be present. It will scan your system for any files or folders that may contain malware and remove them.

6. **Privacy Cleaner** (3 steps). This tool is used to clean up your system and remove any traces of malware. It will scan your system for any files or folders that may contain malware and remove them.

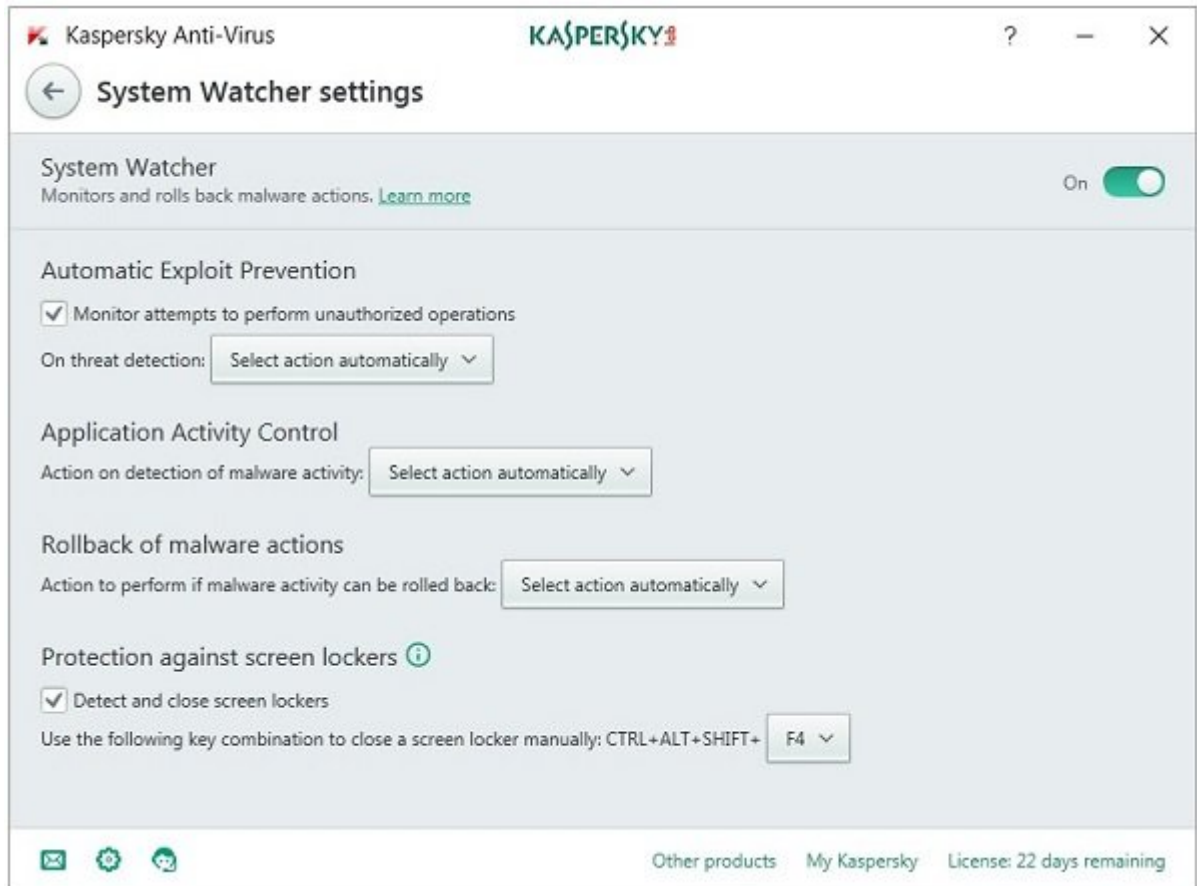
7. **Browser Configuration** (3 steps). This tool is used to configure your web browser to prevent malware from being downloaded or installed. It will scan your browser for any settings that may be vulnerable to malware and configure them to be secure.

8. **Rescue Disk** (3 steps). This is a bootable disk that you can use to scan and remove malware from a computer that is infected. It is a safe mode that allows you to scan and remove malware without the risk of the malware interfering with the scan.

9. **Rescue Mode** (3 steps). This mode is used to scan and remove malware from a computer that is infected. It is a safe mode that allows you to scan and remove malware without the risk of the malware interfering with the scan.



.Microsoft Windows Security notification window showing a detected threat: EICAR-Test-File. The notification advises closing all active programs and saving changes before a computer restart. It provides a link to 'Try to disinfect without computer restart' and a checkbox to 'Apply to all objects of this type'. (9 points)



IM Anti-virus

IM Anti-virus is a feature of Kaspersky Anti-Virus that provides protection against malware and ransomware attacks on your instant messaging (IM) applications. It monitors and blocks suspicious activity, preventing the spread of malicious files and protecting your personal data. This feature is available in the Kaspersky Anti-Virus interface, where you can configure its settings to suit your needs.

IM Anti-virus is a feature of Kaspersky Anti-Virus that provides protection against malware and ransomware attacks on your instant messaging (IM) applications. It monitors and blocks suspicious activity, preventing the spread of malicious files and protecting your personal data. This feature is available in the Kaspersky Anti-Virus interface, where you can configure its settings to suit your needs.

IM Anti-virus is a feature of Kaspersky Anti-Virus that provides protection against malware and ransomware attacks on your instant messaging (IM) applications. It monitors and blocks suspicious activity, preventing the spread of malicious files and protecting your personal data. This feature is available in the Kaspersky Anti-Virus interface, where you can configure its settings to suit your needs.

IM Anti-virus is a feature of Kaspersky Anti-Virus that provides protection against malware and ransomware attacks on your instant messaging (IM) applications. It monitors and blocks suspicious activity, preventing the spread of malicious files and protecting your personal data. This feature is available in the Kaspersky Anti-Virus interface, where you can configure its settings to suit your needs.

IM Anti-virus is a feature of Kaspersky Anti-Virus that provides protection against malware and ransomware attacks on your instant messaging (IM) applications. It monitors and blocks suspicious activity, preventing the spread of malicious files and protecting your personal data. This feature is available in the Kaspersky Anti-Virus interface, where you can configure its settings to suit your needs.

IM Anti-virus is a feature of Kaspersky Anti-Virus that provides protection against malware and ransomware attacks on your instant messaging (IM) applications. It monitors and blocks suspicious activity, preventing the spread of malicious files and protecting your personal data. This feature is available in the Kaspersky Anti-Virus interface, where you can configure its settings to suit your needs. For more information, see the [FAQ](#) page. (12 pages) IM Anti-virus

<https://www.shabakeh-mag.com/security/13766/%DA%A7%D8%B1%D8%A7-%D8%A8%D8%B1-%D8%A7%DB%8C-%D8%AA%D8%A7%D9%85%DB%8C%D9%86-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%DB%8C-%D8%AE%D9%88%D8%AF-%D9%85%DB%8C%E2%80%8C%D8%AA%D9%88%D8%A7%D9%86%DB%8C%D8%AF-%D8%A8%D9%87-%DA%A9%D8%B3%D9%BE%D8%B1%D8%B3%DA%A9%DB%8C-%D8%A7%D8%B9%D8%AA%D9%85%D8%A7%D8%AF-%DA%A9%D9%86%DB%8C%D8%AF%D8%9F>