Да разгледаме информация от „първа ръка“ – сайта на Microsoft на този линк

<https://support.microsoft.com/bg-bg/topic/%D0%B8%D0%B7%D0%B1%D1%8F%D0%B3%D0%B2%D0%B0%D0%BD%D0%B5-%D0%B8-%D0%BF%D1%80%D0%B5%D0%BC%D0%B0%D1%85%D0%B2%D0%B0%D0%BD%D0%B5-%D0%BD%D0%B0-%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%B8-%D0%B8-%D0%B4%D1%80%D1%83%D0%B3-%D0%B7%D0%BB%D0%BE%D0%BD%D0%B0%D0%BC%D0%B5%D1%80%D0%B5%D0%BD-%D1%81%D0%BE%D1%84%D1%82%D1%83%D0%B5%D1%80-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5>

# Ето какво ни съветват специалисти по сигурността:

# Избягване и премахване на вируси и друг злонамерен софтуер

# Какво представлява злонамереният софтуер?

Злонамереният софтуер е термин, който се използва за злонамерен софтуер, който е проектиран да причинява щети или нежелани действия на компютърна система. Примерите за злонамерен софтуер включват следното:

* Вируси
* Червеи
* Троянски коне
* Шпионски софтуер
* Фалшив софтуер за защита

## Какво представлява компютърният вирус?

Компютърният вирус е малка софтуерна програма, която се разпространява от един компютър на друг и пречи на работата на компютъра. Компютърният вирус може да повреди или изтрие данни на компютъра, да използва имейл програма, за да разпространи вируса на други компютри, или дори да изтрие всичко на твърдия диск.  
  
Компютърните вируси често се разпространяват чрез прикачени файлове в имейл съобщения или чрез незабавни съобщения. Затова никога не трябва да отваряте прикачен към имейл файл, освен ако не познавате подателя на съобщението или ако не очаквате прикачения към имейл файл. Вирусите могат да бъдат прикрити под формата на прикачени файлове със забавни изображения, поздравителни картички или аудио- и видеофайлове. Компютърните вируси се разпространяват и чрез файлове за изтегляне от интернет. Те могат да бъдат скрити в пиратски софтуер или в други файлове или програми, които можете да изтегляте.

**Съвет:**За информация относно симптомите на компютърен вирус отидете на уеб сайта [microsoft PC Security.](https://www.microsoft.com/security/portal/mmpc/default.aspx)

## Какво представлява червеят?

Червеят е компютърен код, който се разпространява без взаимодействие с потребителя. Повечето червеи започват като прикачени към имейл файлове, които заразяват компютъра, след като бъдат отворени. Червеят сканира заразения компютър за файлове, като например адресни книги или временни уеб страници, които съдържат имейл адреси. Червеят използва адресите, за да изпраща заразени имейл съобщения, и често имитира (или сменя неправомерно самоличността на) адреси от папката "От" в изпращани след това имейл съобщения, така че тези заразени съобщения да изглеждат, че са от някого, когото познавате. След това червеите се разпространяват автоматично чрез имейл съобщения, мрежи или уязвимости на операционната система, като често завладяват тези системи, преди причината да е станала известна. Червеите не винаги са разрушителни за компютрите, но те обикновено причиняват проблеми с производителността и стабилността на компютри и мрежи.

## Какво представлява троянският кон?

Троянският кон е злонамерена софтуерна програма, която се крие в други програми. Тя влиза в компютъра, скрита зад легитимна програма, като например скрийнсейвър. След това тя въвежда код в операционната система, която позволява на хакер достъп до заразения компютър. Троянските коне обикновено не се разпространяват сами. Те се разпространяват от вируси, червеи или изтеглен софтуер.

## Какво представлява шпионският софтуер?

Шпионският софтуер може да се инсталира на компютъра ви без ваше знание. Тези програми могат да променят конфигурацията на компютъра ви или да събират рекламни данни и лични данни. Шпионският софтуер може да следи навиците за търсене в интернет и може да пренасочва уеб браузъра ви към различен уеб сайт от този, на който сте имали намерение да отидете.

## Какво представлява фалшивият софтуер за защита?

Фалшивата софтуерна програма за защита се опитва да ви накара да мислите, че компютърът ви е заразен с вирус и обикновено ви подтиква да изтеглите или закупите продукт, който премахва вируса. Имената на тези продукти често съдържат думи като Antivirus, Shield, Security, Protection или Fixer. Това ги прави да звучат легитимни. Те често се изпълняват веднага след като ги изтеглите или при следващото стартиране на компютъра. Фалшивият софтуер за защита може да попречи на приложения, като например Internet Explorer, да се отварят. Фалшивият софтуер за защита може също така да покаже легитимни и важни файлове на Windows като заразени. Типичните съобщения за грешка или изскачащите съобщения могат да съдържат следните фрази:

Предупреждение!  
Компютърът ви е заразен!  
Този компютър е заразен от шпионски и рекламен софтуер.

Забележка Ако получите съобщение в изскачащ диалогов прозорец, който прилича на това предупреждение, натиснете ALT + F4 на клавиатурата, за да затворите диалоговия прозорец. Не щракайте върху нищо в диалоговия прозорец. Ако предупреждение, като например това тук, продължава да се показва, когато се опитате да затворите диалоговия прозорец, това е добра индикация, че съобщението е злонамерено.

Наистина ли искате да навигирате от тази страница?  
Компютърът ви е заразен! Те могат да причинят загуба на данни и повреда на файлове и трябва да бъдат третирани възможно най-скоро. Натиснете "Отказ", за да го избегнете. Върнете се към "Защита на системата" и я изтеглете, за да защитите компютъра си.  
Натиснете OK, за да продължите или да отмените, за да останете на текущата страница.

Ако виждате този вид съобщение, не изтегляйте или не купувайте софтуера.

За повече информация вижте [Защита от измами с техническа поддръжка.](https://support.microsoft.com/bg-bg/windows/%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D0%B0%D0%B7%D0%B5%D1%82%D0%B5-%D1%81%D0%B5-%D0%BE%D1%82-%D0%B8%D0%B7%D0%BC%D0%B0%D0%BC%D0%B8-%D1%81-%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0-%D0%BF%D0%BE%D0%B4%D0%B4%D1%80%D1%8A%D0%B6%D0%BA%D0%B0-2ebf91bd-f94c-2a8a-e541-f5c800d18435)

## Премахване на злонамерен софтуер, като вируси, шпионски софтуер или фалшив софтуер за защита

Премахването на компютърен вирус или шпионски софтуер може да бъде трудно без помощта на инструменти за премахване на злонамерен софтуер. Някои компютърни вируси и друг нежелан софтуер се преинсталират сами, след като вирусите и шпионският софтуер са открити и премахнати. За щастие, като актуализирате компютъра и използвате инструменти за премахване на злонамерен софтуер, можете завинаги да премахнете нежелания софтуер.  
  
За повече информация как да премахнете компютърен вирус и шпионски софтуер, вижте следната статия в базата знания на Microsoft: [2671662](http://support.microsoft.com/help/2671662) – ресурси и указания на Microsoft за премахване на злонамерен софтуер и вируси

### Следвайте последователно тези стъпки, за да премахнете компютърния вирус и друг злонамерен софтуер.

### 1. Инсталирайте най-новите актуализации от Microsoft Update

Забележка Компютърен вирус може да ви попречи да получите достъп до уеб сайта на Microsoft Update, за да инсталирате най-новите актуализации. Препоръчваме да настроите услугата за автоматични актуализации да се изпълнява автоматично, така че на компютъра да не липсват никакви важни актуализации.

За повече информация вж. [Windows Актуализация: ЧЗВ](https://support.microsoft.com/bg-bg/windows/windows-update-%D1%87%D0%B7%D0%B2-8a903416-6f45-0718-f5c7-375e92dddeb2)

## Windows 7

### 2. Използвайте безплатния Скенер за безопасност на Microsoft

Microsoft предлага безплатен онлайн инструмент, който сканира и помага за премахване на потенциални заплахи от компютъра ви. За да изпълните сканирането, посетете уеб сайта на [скенера за безопасност на Microsoft](https://www.microsoft.com/security/scanner).

### 3. Използвайте инструмента Windows за премахване на злонамерен софтуер

За повече информация относно инструмента за премахване на злонамерен софтуер на Microsoft вижте следната статия в базата знания на Microsoft:

[890830](http://support.microsoft.com/help/890830) – Премахване на определен преобладаващ злонамерен софтуер с Windows инструмент за премахване на злонамерен софтуер

### 4. Ръчно премахване на злонамерен софтуер за защита

Ако злонамереният софтуер за защита не може да бъде открит или премахнат с помощта Скенер за безопасност на Microsoft или инструмента за премахване Windows злонамерен софтуер, изпробвайте следните стъпки:

## Windows 7

### 5. Стартирайте Microsoft Defender Offline

Microsoft Defender Offline е инструмент против злонамерен софтуер, който помага за премахването на трудни за премахване вируси, които започват преди Windows стартира. Започвайки от Windows 10, Microsoft Defender Offline е вграден. За да го използвате, следвайте стъпките в тази статия: [Помогнете за защитата на моя компютър с Microsoft Defender Offline.](https://support.microsoft.com/bg-bg/windows/%D0%BF%D0%BE%D0%B4%D0%BE%D0%B1%D1%80%D1%8F%D0%B2%D0%B0%D0%BD%D0%B5-%D0%BD%D0%B0-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%B0-%D1%81-microsoft-defender-offline-9306d528-64bf-4668-5b80-ff533f183d6c)

## Windows 7 или Windows 8

## Защита на компютъра ви от злонамерен софтуер

Има действия, които можете да предприемете, за да защитите компютъра си от злонамерен софтуер.

### Включване на защитната стена

Уверете се, че Windows защитната стена е включена. Вижте [Включване или изключване на защитната стена на Microsoft Defender](https://support.microsoft.com/bg-bg/windows/%D0%B2%D0%BA%D0%BB%D1%8E%D1%87%D0%B2%D0%B0%D0%BD%D0%B5-%D0%B8-%D0%B8%D0%B7%D0%BA%D0%BB%D1%8E%D1%87%D0%B2%D0%B0%D0%BD%D0%B5-%D0%BD%D0%B0-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%BD%D0%B0%D1%82%D0%B0-%D1%81%D1%82%D0%B5%D0%BD%D0%B0-%D0%BD%D0%B0-microsoft-defender-ec0844f7-aebd-0583-67fe-601ecf5d774f) за инструкции как да направите това в модерните версии на Windows.

## Windows 7

### Поддържайте компютъра си актуализиран

За повече информация как да зададете автоматични актуализации в Windows, [вижте Windows: ЧЗВ](https://support.microsoft.com/bg-bg/windows/windows-update-%D1%87%D0%B7%D0%B2-8a903416-6f45-0718-f5c7-375e92dddeb2)

### Не се подлъгвайте да изтегляте злонамерен софтуер

Ето някои съвети, които могат да ви предпазят от изтеглянето на софтуер, който не искате:

* Изтегляйте само програми от сайтове, на които имате доверие. Ако не сте сигурни дали да се доверите на програма, която искате да изтеглите, въведете името на програмата във вашата любима търсачка, за да видите дали някой друг е съобщил, че съдържа шпионски софтуер.
* Прочитайте всички предупреждения за защита, лицензионни договори и декларации за поверителност, които са свързани с всеки софтуер, който изтегляте.
* Никога не щракайте върху "Приемам" или "OK", за да затворите прозорец, за който подозирате, че може да е шпионски софтуер. Вместо това щракнете върху червения "x" в ъгъла на прозореца или натиснете Alt + F4 на клавиатурата, за да затворите прозореца.
* Внимавайте с популярните "безплатни" програми за споделяне на файлове с музика и филми и се уверете, че разбирате целият софтуер, който идва с тези програми.
* Използвайте стандартен потребителски акаунт вместо акаунт на администратор. Акаунтът на администратор има достъп до всичко в системата, а всеки злонамерен софтуер, изпълняван с акаунт на администратор, може да използва разрешенията на администратора, за да може да зарази или повреди всички файлове в системата.

За повече информация как да защитите компютър от вируси, вижте [Защита на моя компютър от](https://support.microsoft.com/bg-bg/windows/%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%B0-%D0%BE%D1%82-%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%B8-b2025ed1-02d5-1e87-ba5f-71999008e026)