F-Secure Anti-Virus 2013

Съдържание

Глава 1: Инсталиране.....5

Преди да инсталирате за пръв път.....6
Инсталиране на продукта за първи път.....6
Исталиране и надстройване на приложения.....6
Помощ и поддръжка.....7

Глава 2: Първи стъпки.....9

Как се използват автоматичните актуализации.....10
Проверка на състоянието на актуализация.....10
Промяна на настройките за интернет връзка.....10
Проверка на състоянието на мрежата за защита в реално време.....11
Как да видя какво е направила програмата.....11
Преглед на хронология на известията.....11
Промяна на настройките за известия.....11
Мрежа за защита в реално време.....12
Какво представлява Мрежата за защита в реално време.....12
Ползи от Мрежата за защита в реално време.....12
Какви данни предоставяте.....13
Как защитаваме вашите поверителни данни.....14
Как да станете участник в Мрежата за защита в реално време.....15
Въпроси за Мрежата за защита в реално време.....15
Как да разбера дали абонаментът ми е валиден.....15
Работен център.....16
Активиране на абонамент.....16

Глава 3: Въведение.....17

Преглед на общото състояние на моята защита.....18
Преглед на статистика на продукта.....18
Боравене с актуализации на продукта.....19
Преглед на версии на база данни.....19
Променете настройките за мобилна широколентова връзка.....19
Какво представляват вирусите и другият злонамерен софтуер.....20
Вируси.....20
Шпиониращ софтуер.....21
Комплекти за пълен достъп.....21
Рисков софтуер.....21

Глава 4: Защита на компютъра от злонамерен софтуер.....23
Как да сканирам своя компютър.....24
Автоматично сканиране на файлове.....24
Ръчно сканиране на файлове.....26
Сканиране на имейл.....29
Преглед на резултатите от сканирането.....30
Как да се изключат файлове от сканирането.....31
Изключване на типове файлове.....31
Изключване на файлове според местоположение.....31
Преглед на изключени приложения.....32
Как се използва карантината.....33
Преглед на поставените под карантина елементи.....33
Възстановяване на поставени под карантина елементи.....34
Какво представлява DeepGuard.....34
Включване и изключване на DeepGuard.....34
Позволяване на приложения, блокирани от DeepGuard.....35
Използване на DeepGuard в режим на съвместимост.....35
Какво да правите с предупреждения за подозрително поведение.....35

Глава

1

Инсталиране

Теми:

- *Преди да инсталирате за пръв път*
- *Инсталиране на продукта за първи път*
- *Исталиране и надстройване на приложения*
- *Помощ и поддръжка*

Преди да инсталирате за пръв път

Благодарим ви, че избрахте F-Secure.

За да инсталирате продукта, се нуждаете от следното:

- Инсталационен компактдиск или инсталационен пакет. Ако използвате нетбук без CD устройство, можете да изтеглите инсталационния пакет от *www.f-secure.com/netbook*.
- Ключ за абонамент.
- Връзка към интернет.

Ако имате продукт за защита от друг доставчик, инсталационната програма ще се опита да го премахне автоматично. Ако това не стане, премахнете го ръчно.

Бележка: Ако имате повече от един акаунт на компютъра, влезте с привилегии на администратор, когато инсталирате.

Инсталиране на продукта за първи път

Инструкции за инсталиране на продукта.

Изпълнете следните инструкции, за да инсталирате продукта:

1. Поставете компактдиска или щракнете двукратно върху инсталиращата програма, която сте изтеглили.

   Ако компактдискът не стартира автоматично, отидете в Windows Explorer, щракнете двукратно върху иконата на CD-ROM устройството и щракнете двукратно върху инсталационния файл, за да стартирате инсталирането.

2. Следвайте инструкциите на екрана.

   - Ако сте закупили продукта на компактдиск от магазин, можете да намерите ключа за абониране на корицата на ръководството за бързо инсталиране.
   - Ако сте изтеглили продукта от F-Secure eStore, ключът за абониране е включен в имейла за потвърждение на поръчката за покупка.

   Възможно е да е необходимо рестартиране на вашия компютър преди да валидирате вашия абонамент и да изтеглите най-новите актуализации от интернет. Ако инсталирате от компактдиска, не забравяйте да извадите инсталационния компактдиск от устройството, преди да рестартирате вашия компютър.

Исталиране и надстройване на приложения

Инструкции за активиране на вашия нов абонамент.

Следвайте тези инструкции, за да активирате вашия нов абонамент или за да инсталирате ново приложение, като използвате стартовата площадка:

Бележка: Можете да намерите иконата на стартовата площадка в системната област на Windows.

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.

2. Изберете **Преглед на моите абонаменти**.
3. В **Моите абонаменти** отидете на страницата **Състояние на абонаменти** и щракнете върху **Активиране на абонамент**.
   Отваря се прозорец **Активиране на абонамент**.
4. Въведете вашия ключ за абонамент за приложението и щракнете върху **OK**.
5. След като вашият абонамент бъде валидиран и активиран, щракнете върху **Затвори**.
6. В **Моите абонаменти** отидете на страницата **Състояние на инсталация**. Ако инсталирането не започне автоматично, следвайте тези инструкции:
   a) Щракнете върху **Инсталиране**.
      Отваря се прозорецът за инсталиране.
   b) Щракнете върху **Напред**.
      Приложението се изтегля и инсталирането започва.
   c) Когато инсталирането завърши, щракнете върху **Затвори**.

Новият абонамент се активира.

Помощ и поддръжка

Можете да осъществите достъп до помощ за продукта онлайн като щракнете върху иконата "Помощ" или натиснете F1 в който и да е екран на продукта.

След като регистрирате вашия лиценз, имате право на допълнителни услуги, като безплатни актуализации на продукта и поддръжка на продукта. Можете да се регистрирате на *www.f-secure.com/register*.

Глава

2

Първи стъпки

Теми:

- *Как се използват автоматичните актуализации*
- *Как да видя какво е направила програмата*
- *Мрежа за защита в реално време*
- *Как да разбера дали абонаментът ми е валиден*

Информация как да направите първите стъпки в продукта.

В този раздел е описано как да промените общите настройки и да управлявате вашите абонаменти през стартовата площадка.

Общите настройки на стартовата площадка са настройки, които важат за всички програми, инсталирани на стартовата площадка. Вместо да променяте настойките поотделно във всяка програма, можете просто да редактирате общите настройки, които след това се използват от всички инсталирани програми.

Общите настройки на стартовата площадка включват:

- Изтегляния, където можете да видите информация за това какви актуализации са изтеглени и да проверите ръчно дали има налични нови актуализации.
- Настройки за връзка, където можете да промените начина на свързване на вашия компютър към интернет.
- Известия, където можете да прегледате предишни известия и да настроите какви известия искате да виждате.
- Настройки за поверителност, където можете да изберете дали на вашия компютър е позволено да се свързва с Мрежата за защита в реално време.

Можете да управлявате вашите абонаменти за инсталирани програми също и чрез стартовата площадка.

Как се използват автоматичните актуализации

Автоматичните актуализации поддържат защитата на вашия компютър актуализирана.

Продуктът извлича най-новите актуализации на компютъра ви, когато сте свързани с интернет. Той установява какъв е мрежовият трафик и не пречи на останалото използване на интернет дори при бавна интернет връзка.

Проверка на състоянието на актуализация

Прегледайте датата и часа на най-новата актуализация.

Когато са включени автоматичните актуализации, продуктът автоматично получава най-новите актуализации, когато сте свързвани с интернет.

За да се уверите, че имате най-новите актуализации:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Отваряне на общи настройки**.
3. Изберете **Автоматични актуализации** > **Изтегляния**.
4. Щракнете върху **Проверка сега**.
   Продуктът се свързва с интернет и проверява за най-новите актуализации. Ако защитата не е актуализирана, той извлича най-новите актуализации.

   Бележка: Ако използвате модем или имате ISDN връзка с интернет, връзката трябва да е активна, за да се извърши проверка за актуализации.

Промяна на настройките за интернет връзка

Обикновено няма никаква нужда да променяте настройките по подразбиране, но можете да конфигурирате как сървърът се свързва с интернет, така че да можете автоматично да получавате актуализации.

За да промените настройките за интернет връзка:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Отваряне на общи настройки**.
3. Изберете **Автоматични актуализации** > **Връзка**.
4. В списъка **Интернет връзка** изберете как вашият компютър е свързан с интернет.
   - Изберете **Предполагане на постоянно свързване**, ако имате постоянна мрежова връзка.

     Бележка: Ако компютърът ви всъщност няма постоянна мрежова връзка и е настроен за комутируема връзка при поискване, избирането на **Предполагане на постоянно свързване** може да доведе до множество набирания.
   - Изберете **Откриване на свързване**, за да се извличат актуализации, когато продуктът открие активна мрежова връзка.
   - Изберете **Откриване на трафик**, за да се извличат актуализации само когато продуктът открие друг мрежов трафик.

     Съвет: Ако имате рядко срещана хардуерна конфигурация, която става причина настройката **Откриване на свързване** да открива активна мрежова връзка дори когато няма такава, вместо нея изберете **Откриване на трафик**.

5. В списъка **HTTP прокси** изберете дали компютърът ви използва *прокси сървър* за свързване с интернет.
   - Изберете **Без HTTP прокси**, ако компютърът ви е свързан директно с интернет.
   - Изберете **Ръчно конфигуриране на HTTP прокси**, за да конфигурирате настройките на *HTTP прокси сървъра*.
   - Изберете **Използване на HTTP прокси на моя браузър**, за да използвате същите настройки за *HTTP прокси* сървър, които сте конфигурирали във вашия уеб браузър.

Проверка на състоянието на мрежата за защита в реално време

За да функционират правилно, много компоненти на продукта зависят от възможностите за свързване на мрежата за защита в реално време.

Ако има мрежови проблеми или ако защитната стена блокира трафика на мрежата за защита в реално време, състоянието е "изключена". Ако не са инсталирани компоненти на продукта, които да изискват достъп до мрежата за защита в реално време, състоянието е "не се използва".

За да проверите състоянието:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Отваряне на общи настройки**.
3. Изберете **Автоматични актуализации** > **Връзка**.

Под "**Мрежа за защита в реално време**" можете да видите текущото състояние на мрежата за защита в реално време.

Как да видя какво е направила програмата

На страницата **Известия** можете да видите какви действия е предприел продукта за защита на вашия компютър.

Когато предприеме действие, продуктът ще покаже известие, например когато намери вирус, който блокира. Някои известия могат да бъдат изпратени от вашия доставчик на услуги, например за да ви уведоми, че се предлагат нови услуги.

Преглед на хронология на известията

В хронологията на известията можете да видите какви известия са били показвани

За да прегледате хронологията на известията:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Отваряне на общи настройки**.
3. Изберете **Други** > **Известия**.
4. Щракнете върху **Показване на хронология на известията**. Отваря се списък на хронологията на известията.

Промяна на настройките за известия

Можете да изберете какъв тип известия искате да показва продуктът.

За да промените настройките за известия:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Отваряне на общи настройки**.
3. Изберете **Други** > **Известия**.
4. Отметнете или изчистете отметката от **Позволяване на програмни съобщения**, за да включите или изключите програмните съобщения.

   Когато тази настройка е включена, продуктът ще показва съобщения от инсталираните програми.
5. Отметнете или изчистете отметката от **Позволяване на промоционални съобщени**я, за да включите или изключите промоционалните съобщения.
6. Щракнете върху **OK**.

Мрежа за защита в реално време

Този документ описва Мрежата за защита в реално време, онлайн услуга на F-Secure Corporation, която идентифицира чисти приложения и уеб сайтове, като същевременно осигурява защита срещу злонамерен софтуер и троянски коне от уеб сайтове.

Какво представлява Мрежата за защита в реално време

Мрежата за защита в реално време е онлайн услуга, която предоставя бърз отговор срещу най-новите базирани на интернет заплахи.

Като участник в Мрежата за защита в реално време, вие можете да ни помогнете да засилим защитата срещу нови и възникващи заплахи. Мрежата за защита в реално време събира статистика за определени непознати, злонамерени или подозрителни приложения и за това какво правят те на вашето устройство. Тази информация е анонимна и се изпраща на F-Secure Corporation за комбиниран анализ на данните. Ние използваме анализираната информация, за да подобрим защитата на вашето устройство срещу най-новите заплахи и злонамерени файлове.

Как работи Мрежата за защита в реално време

Като участник в Мрежата за защита в реално време, вие можете да предоставите информация за непознати приложения и уеб сайтове, и за злонамерени приложения и троянски коне от уеб сайтове. Мрежата за защита в реално време не проследява вашата дейност в мрежата и не събира информация за уеб сайтове, които вече са били анализирани, както и не събира информация за чисти приложения, които са инсталирани на вашия компютър.

Ако не желаете да допринасяте с такива данни, Мрежата за защита в реално време няма да събира информация за инсталирани приложения или посещавани уеб сайтове. Продуктът обаче е необходимо да отправя запитвания до сървърите на F-Secure за репутацията на приложения, уеб сайтове, съобщения и други обекти. Запитването се извършва като се използва криптографска контролна сума, като обектът на запитването не се изпраща до F-Secure. Ние не проследяваме данните по потребители; само броячът на файла или уеб сайта се увеличава с единица.

Не е възможно да се спре целият мрежов трафик за Мрежата за защита в реално време, тъй като тя е съставна част от защитата, предоставяна от продукта.

Ползи от Мрежата за защита в реално време

С Мрежата за защита в реално време ще имате по-бърза и по-адекватна защита срещу най-новите заплахи и няма да получавате излишни предупреждения за подозрителни приложения, които не са злонамерени.

Като участник в Мрежата за защита в реално време, можете да ни помогнете да откриваме нов и неоткрит злонамерен софтуер и да премахваме възможните грешни положителни резултати от нашата база данни с дефиниции на вируси.

Всички участници в Мрежата за защита в реално време си помагат един на друг. Когато Мрежата за защита в реално време открие подозрително приложение на вашето устройство, вие извличате полза от резултатите от анализа когато същото приложение вече е било открито на други устройства. Мрежата за защита в реално време подобрява общата производителност на вашето устройство, тъй като инсталираният продукт за защита не е необходимо да сканира приложения, които Мрежата за защита в реално време вече е анализирала и е установила, че са чисти. Аналогично, информацията за злонамерени уеб сайтове и нежелани групови съобщения се споделя чрез Мрежата за защита в реално време и ние можем да ви осигурим по-точна защита срещу троянски коне от уеб сайтове и спам.

Колкото повече хора участват в Мрежата за защита в реално време, толкова по-добре са защитени отделните участници.

Какви данни предоставяте

Като участник в Мрежата за защита в реално време вие предоставяте информация за приложения съхранявани на вашето устройство и уеб сайтовете, които посещавате, за да може Мрежата за защита в реално време да осигури защита срещу най-новите злонамерени приложения и подозрителни уеб сайтове.

Анализиране на репутацията на файл

Мрежата за защита в реално време събира информация само за приложения, които нямат позната репутация и за файлове, които са подозрителни или известни като злонамерен софтуер.

Мрежата за защита в реално време събира анонимна информация за чисти или подозрителни приложения на вашето устройство. Мрежата за защита в реално време събира информация само за изпълними файлове (като преносими изпълними файлове на платформата Windows, които имат разширения .cpl, .exe, .dll, .ocx, .sys, .scr и .drv).

Събраната информация включва:

- пътя до файла, където се намира приложението във вашето устройство,
- размера на файла и кога е създаден или променен,
- атрибути и привилегии на файла,
- информация за подписа на файла,
- текущата версия на файла и фирмата, която го е създала,
- произход на файла или URL адрес, от който е изтеглен,
- резултати за сканирани файлове от F-Secure DeepGuard и антивирусен анализ и
- друга подобна информация.

Мрежата за защита в реално време никога не събира информация за вашите лични документи, освен ако не бъде установено, че са инфектирани. По отношение на всеки тип злонамерен файл тя събира името на инфекцията и състоянието на дезинфектиране на файла.

С Мрежата за защита в реално време можете също така да представяте подозрителни приложения за анализ. Приложенията, които представяте, могат да включват само преносими изпълними файлове. Мрежата за защита в реално време никога не събира информация за вашите лични документи и те никога не се качват автоматично за анализ.

Представяне на файлове за анализ

С Мрежата за защита в реално време можете също така да представяте подозрителни приложения за анализ.

Можете да представяте отделни подозрителни приложения ръчно, когато продуктът ви подкани да направите това. Можете да представяте само преносими изпълними файлове. Мрежата за защита в реално време никога не качва ваши лични документи.

Анализиране на репутация на уеб сайт

Мрежата за защита в реално време не проследява вашата дейност в уеб и не събира информация за уеб сайтове, които са вече анализирани. Тя се уверява, че посещаваните уеб сайтове са безопасни, докато сърфирате в мрежата. Когато посещавате даден уеб сайт, Мрежата за защита в реално време проверява неговата безопасност и ви известява, ако степента на безопасност е подозрителна или опасна.

Ако уеб сайтът, който посещавате, съдържа злонамерено или подозрително съдържание или известен троянски кон, Мрежата за защита в реално време събира целия URL адрес на сайта, за да може да бъде анализирано съдържанието на уеб страницата.

Ако посетите сайт, който още не е оценен, Мрежата за защита в реално време събира имена на домейни и поддомейни, а в някои случаи и пътя до посещаваната страница, за да може сайтът да бъде анализиран и оценен. Всички параметри на URL, които е вероятно да съдържат информация, която може да бъде свързана с вас във формат за личностно идентифициране, се премахват с цел защита на вашата поверителност.

Бележка: Мрежата за защита в реално време не оценява и не анализира уеб страници в частни мрежи, затова никога не събира информация за IP адреси в частни мрежи (например корпоративен интранет).

Анализиране на системна информация

Мрежата за защита в реално време събира името и версията на вашата операционна система, информация за интернет връзката и статистика за използването на Мрежата за защита в реално време (например колко пъти са отправяни запитвания за репутация на уеб сайт и средното време, за което запитването е върнало резултат), за да можем да наблюдаваме и подобряваме услугата.

Как защитаваме вашите поверителни данни

Ние прехвърляме информацията безопасно и автоматично премахваме всякаква лична информация, която може да се съдържа в данните.

Мрежата за защита в реално време премахва данни за идентификация, преди да ги изпрати до F-Secure, и шифрова цялата събрана информация по време на трансфера, за да я предпази от непозволен достъп. Събраната информация не се обработва поотделно; тя се групира с информация от други участници в Мрежата за защита в реално време. Всички данни се анализират статистически и анонимно, което означава, че никакви данни няма да бъдат свързани с вас по никакъв начин.

Цялата информация, която може да ви идентифицира лично, не се включва в събраните данни. Мрежата за защита в реално време не събира IP адреси или друга поверителна информация, като адреси на имейли, потребителски имена и пароли. Макар че полагаме всички усилия да премахваме всички данни за лично идентифициране, възможно е някои данни за идентификация да останат в събраната информация. В такива случаи ние няма да се стремим да използваме такива неумишлено събрани данни, за да ви идентифицираме.

Ние прилагаме стриктни мерки за защита и физически, административни и технически предпазни мерки, за да защитим събраната информация при прехвърлянето, съхраняването и обработването ѝ. Информацията се съхранява на защитени места и на сървъри контролирани от нас, разположени или в нашите офиси, или в офиси на наши подизпълнители. Само персонал с правомощия може да има достъп до събраната информация.

F-Secure може да споделя събраната информация със свои дъщерни фирми, подизпълнители, дистрибутори и партньори, но винаги във формат, в който не може да бъде идентифицирана и е анонимна.

Как да станете участник в Мрежата за защита в реално време

Вие ни помагате да подобрим защитата чрез Мрежата за защита в реално време, като допринасяте информация за злонамерени програми и уеб сайтове.

Можете да изберете дали да участвате в Мрежата за защита в реално време по време на инсталирането. При настройките по подразбиране на инсталирането вие допринасяте данни за Мрежата за защита в реално време. Можете да промените тази настройка по-късно в продукта.

Следвайте тези инструкции, за да промените настройките за Мрежата за защита в реално време:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Отваряне на общи настройки**.
3. Изберете **Други** > **Поверителност**.
4. Поставете отметка в квадратчето за участие, за да станете участник в Мрежата за защита в реално време.

Въпроси за Мрежата за защита в реално време

Информация за връзка за въпроси относно Мрежата за защита в реално време.

Ако имате допълнителни въпроси за Мрежата за защита в реално време, свържете се с:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

Последната версия на това правило е винаги на разположение на нашия уеб сайт.

Как да разбера дали абонаментът ми е валиден

Типът и състоянието на абонамента ви е показан на страницата **Състояние на абонамент**.

Когато срокът на абонамента предстои да изтече или вашият абонамент е изтекъл, цялостното състояние на защитата на програмата в съответната икона на стартовата площадка се променя.

За да проверите валидността на абонамента:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Преглед на моите абонаменти**.
3. Изберете **Състояние на абонаменти**, за да видите информация за вашите абонаменти за инсталирани програми.
4. Изберете **Състояние на инсталация**, за да видите налични програми за инсталиране.

Състоянието и датата на изтичане на вашия абонамент се показват и на страницата **Статистика** на програмата. Ако абонаментът ви е изтекъл, трябва да го подновите, за да продължите да получавате актуализации и да използвате продукта.

Бележка: Когато абонаментът ви е изтекъл, иконата за състояние на продукта мига в системната област.

Работен център

Работният център ви показва важни известия, които изискват вашето внимание.

Ако срокът на вашия абонамент е изтекъл или предстои да изтече, работният център ви известява за това. Фоновият цвят и съдържанието на известието от работния център зависят от типа и състоянието на вашия абонамент:

- Ако срокът на вашия абонамент предстои да изтече и има налични свободни абонаменти, съобщението е на бял фон и има бутон **Активиране**.
- Ако срокът на вашия абонамент предстои да изтече и няма свободни абонаменти, съобщението е на жълт фон и има бутони **Купуване** и **Enter**. Ако вече сте закупили нов абонамент, можете да щракнете върху **бутона Enter**, за да предоставите ключа за абонамент и да активирате вашия нов абонамент.
- Ако срокът на вашия абонамент е изтекъл и има налични свободни абонаменти, съобщението е на червен фон и има бутон **Активиране**.
- Ако срокът на вашия абонамент е изтекъл и няма свободни абонаменти, съобщението е на червен фон и има бутони **Купуване** и **Ente**r. Ако вече сте закупили нов абонамент, можете да щракнете върху **бутона Enter**, за да предоставите ключа за абонамент и да активирате вашия нов абонамент.

Бележка: Връзката **Показване на хронология на известия** в работния център показва списък на известия на продукта, а не предишни съобщения от работния център.

Активиране на абонамент

Когато имате нов ключ за абонамент или ключ за кампания, необходимо е да го активирате.

За да активирате абонамент:

1. На стартовата площадка щракнете с десния бутон на мишката върху най-дясната икона. Появява се изскачащо меню.
2. Изберете **Преглед на моите абонаменти**.
3. Изберете едно от следните:
   - Щракнете върху **Активиране на абонамент**.
   - Щракнете върху **Активиране на код за кампания**.
4. В диалоговия прозорец, който се отваря, въведете вашия нов ключ за абонамент или ключ за кампания и щракнете върху **OK**.

   Съвет: Ако сте получили ключа за абониране по имейл, можете да копирате ключа от имейл съобщението и да го поставите в полето.

След като въведете новия ключ за абонамент, датата на валидността на новия абонамент се показва в страницата **Състояние на абонамент**.

Глава

3

Въведение

Теми:

- *Преглед на общото състояние на моята защита*
- *Преглед на статистика на продукта*
- *Боравене с актуализации на продукта*
- *Какво представляват вирусите и другият злонамерен софтуер*

Този продукт защитава компютъра ви от вируси и други опасни приложения.

Той сканира файлове, анализира приложения и се актуализира автоматично. Не се изискват действия от ваша страна.

Преглед на общото състояние на моята защита

Страницата **Състояние** ви показва бърз преглед на инсталираните компоненти на продукта и тяхното текущо състояние.

За да отворите страницата **Състояние**:

На главната страница щракнете върху **Състояние**.

Отваря се страницата **Състояние**.

Иконата ви показва състоянието на програмата и нейните компоненти за защита.

Икона за състояние	Име на състоянието	Описание
	OK	Компютърът ви е защитен. Компонентът е включен и работи правилно.
	Информация	Продуктът ви информира за специално състояние на компонент. Например функцията се актуализира.
	Предупреждение	Компютърът ви не е напълно защитен. Например продуктът не е бил актуализиран дълго време или състоянието на функцията се нуждае от внимание.
	Грешка	Компютърът ви не е защитен. Например абонаментът ви е изтекъл или критична функция е била изключена.
	Изкл.	Изключен е компонент, който не е критичен.

Преглед на статистика на продукта

Можете да видите какво е направил продуктът след инсталирането му на страницата **Статистика**.

За да отворите страницата **Статистика**:

На главната страница щракнете върху **Статистика**.

Отваря се страницата **Статистика**.

- **Последна успешна проверка за актуализации** показва времето на последната актуализация.

- **Сканиране за вируси и шпиониращ софтуер** показва колко файла е сканирал и изчистил след инсталирането продуктът.
- **Приложения** показва колко програми е разрешил или блокирал DeepGuard след инсталирането.
- **Връзки на защитната стена** показва броя позволени и блокирани връзки от инсталирането насам.
- **Филтър срещу спам и фишинг** показва колко имейл съобщения са били посочени като валидни и като спам.

Боравене с актуализации на продукта

Продуктът автоматично актуализира защитата.

Преглед на версии на база данни

Можете да видите часа на последните актуализации и номерата на версия на страницата **Актуализации на базата данни**.

За да отворите страницата **Актуализации на базата данни**:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Други настройки** > **Версии на базата данни**.

Страницата **Версии на базата данни** показва последната дата, на която дефинициите на вируси и шпиониращ софтуер, DeepGuard и филтрите срещу спам и фишинг са били актуализирани, както и номерата на версиите им.

Променете настройките за мобилна широколентова връзка

Изберете дали искате да изтегляте актуализациите на защитата, когато използвате мобилна широколентова връзка.

Бележка: Тази функция е достъпна само в Microsoft Windows 7.

По подразбиране, актуализациите на защитата винаги се изтеглят когато сте в домашната мрежа на вашия оператор. Актуализациите обаче се спират временно, когато посещавате мрежата на друг оператор. Това е така, защото цените за свързване на различните оператори са различни, например в различните държави. Бихте могли да помислите и да оставите тази настройка непроменена, ако искате да спестите използването на честотната лента, а също така вероятно и разходи, по време на вашето посещение.

Бележка: Тази настройка важи само за мобилни широколентови връзки. Когато компютърът ви е свързан към наземна или безжична мрежа, продуктът се актуализира автоматично.

За да промените настройката:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Други настройки** > **Мобилна широколентова** > **Изтегляне на актуализации на защитата**.
3. Изберете предпочитана опция за актуализация за мобилни връзки:
   - **Само в домашната мрежа на моя оператор**

Актуализациите винаги се изтеглят в домашната мрежа на вашия оператор. Когато посещавате мрежа на друг оператор, актуализациите временно се спират. Препоръчваме да изберете тази опция, за да поддържате вашия продукт за сигурност актуален при очаквани разходи.

- **Никога**

  Актуализациите не се изтеглят, когато използвате мобилна широколентова.

- **Винаги**

  Актуализациите се изтеглят винаги, независимо от мрежата, която използвате. Изберете тази опция, ако искате да сте сигурни, че защитата на вашия компютър е винаги актуална, независимо от разходите.

4. Ако искате да решавате отделно при всяко излизане от домашната мрежа на вашия оператор, изберете **Питай ме всеки път при напускане на домашната мрежа на моя оператор**.

Временно спрени актуализации на защитата

Актуализациите на защитата могат да бъдат временно спрени, когато използвате мобилна широколентова връзка извън домашната мрежа на вашия оператор.

В такъв случай можете да видите листовка за известие **Временно спрени** в долния десен ъгъл на вашия екран. Актуализациите са временно спрени, защото цените за свързване на различните оператори са различни, например в различните държави. Бихте могли да помислите и да оставите тази настройка непроменена, ако искате да спестите използването на честотната лента, а също и разходи, по време на вашето посещение. Обаче ако все пак искате да промените настройките, щракнете върху връзката **Промяна**.

Бележка:

Тази функция е достъпна само в Microsoft Windows 7.

Какво представляват вирусите и другият злонамерен софтуер

Злонамереният софтуер представлява програма, която е специално проектирана така, че да повреди компютъра ви, да използва компютъра ви за незаконни цели без знанието ви или да открадне информация от него.

Злонамереният софтуер може да:

- поеме контрола над вашия уеб браузър;
- пренасочи опитите ви за търсене;
- покаже нежелани реклами;
- проследи уеб сайтовете, които посещавате;
- открадне лични данни, като например банкова информация;
- използва компютъра ви за изпращане на спам и
- използва компютъра ви за атакуване на други компютри.

Злонамереният софтуер може също да стане причина компютърът ви да е по-бавен и нестабилен. Можете да заподозрете наличието на *злонамерен софтуер* на компютъра, ако той внезапно стане много бавен и често се срива.

Вируси

Вирусите обикновено са програми, които могат да се прикачват към файлове и да се реплицират многократно; те могат да променят и заместват съдържанието на други файлове по начин, който може да повреди компютъра ви.

Вирусът е програма, която обикновено се инсталира на компютъра ви без вашето знание. След като вече е попаднал в него, вирусът се опитва да се реплицира. Вирусът:

- използва част от системните ресурси на вашия компютър;
- може да промени или повреди файлове на компютъра ви;
- вероятно използва компютъра ви за инфектиране на други компютри;
- може да позволи използването на компютъра ви за незаконни цели.

Шпиониращ софтуер

Шпиониращият софтуер представлява програми, които събират личните ви данни.

Шпиониращият софтуер може да събира следните лични данни:

- интернет сайтове, които сте разглеждали;
- имейл адреси от вашия компютър;
- пароли или
- номера на кредитни карти.

Шпиониращият софтуер почти винаги се самоинсталира без изричното ви разрешение. Шпиониращият софтуер може да се инсталира с полезна програма или като ви подведе да щракнете върху опция в подвеждащ изскачащ прозорец.

Комплекти за пълен достъп

Комплектите за пълен достъп са програми, които затрудняват откриването на друг *злонамерен софтуер*.

Комплектите за пълен достъп скриват файлове и процеси. По принцип целта им е да прикрият злонамерена дейност на вашия компютър. Когато комплект за пълен достъп крие *злонамерен софтуер*, не можете лесно да откриете, че на компютъра ви има такъв.

Този продукт има скенер за комплекти за пълен достъп, който специално ги търси, така че *злонамереният софтуер* да не може лесно да се скрие.

Рисков софтуер

Рисковият софтуер не е проектиран специално, за да навреди на компютъра ви, но може да му навреди, ако не се използва правилно.

Рисковият софтуер честно казано не е точно зловреден софтуер. Рисковите програми извършват някои полезни, но потенциално опасни функции.

Примери за рискови програми са:

- програми за незабавни съобщения, като IRC (Internet Relay Chat);
- програми за прехвърляне на файлове по интернет от един компютър на друг;
- програми за интернет телефон, като VoIP (*глас по IP протокол*);
- софтуер за отдалечен достъп, като VNC;
- фалшив антивирусен софтуер, който може да подплаши или измами потребители да закупят измамен софтуер за защита или
- софтуер, създаден за избягване на проверки на компактдискове или защити за копиране.

Ако целенасочено сте инсталирали програмата и сте я настроили правилно, е по-малко вероятно тя да е опасна.

Ако рисковият софтуер е инсталиран без знанието ви, е по-вероятно той да е инсталиран с лоши намерения и трябва да бъде премахнат.

Глава

4

Защита на компютъра от злонамерен софтуер

Теми:

- *Как да сканирам своя компютър*
- *Как да се изключат файлове от сканирането*
- *Как се използва карантината*
- *Какво представлява DeepGuard*

Сканирането за вируси и шпиониращ софтуер защитава компютъра от програми, които могат да откраднат лични данни, да повредят сървъра или да го използват за незаконни цели.

По подразбиране всички типове злонамерен софтуер се обработват веднага, щом бъдат открити, така че да не могат да предизвикат вреда.

По подразбиране сканирането за вируси и шпиониращ софтуер автоматично сканира всички ваши локални твърди дискове, преносими носители (например преносими устройства или компактдискове) и изтеглено съдържание. Можете да го настроите така, че да сканира автоматично и имейлите ви.

Сканирането за вируси и шпиониращ софтуер освен това наблюдава компютъра за всякакви промени, които може да са показател за *злонамерен софтуер*. Ако има някакви опасни промени в системата, като например системни настройки или опити за промяна на важни системни процеси, DeepGuard спира работата на тази програма, тъй като има вероятност да е *злонамерен софтуер*.

Как да сканирам своя компютър

Когато е включено сканирането за вируси и шпиониращ софтуер, компютърът ви се сканира автоматично за опасни файлове.

Препоръчваме да оставяте сканирането за вируси и шпиониращ софтуер включено през цялото време. Сканирайте файловете си ръчно, за да се уверите, че на компютъра ви няма опасни файлове или за да сканирате файловете, изключени от сканирането в реално време.

При настройване на планирано сканиране, Сканирането за вируси и шпиониращ софтуер отстранява опасни файлове от компютъра ви в зададените часове.

Автоматично сканиране на файлове

Сканирането в реално време защитава компютъра, като сканира всички файлове, когато до тях се осъществява достъп, и блокира достъпа до тези от тях, които съдържат *злонамерен софтуер*.

Когато компютърът ви опита достъп до файл, сканирането в реално време сканира файла за злонамерен софтуер, преди да позволи достъп до него. Ако сканирането в реално време открие опасно съдържание, то ще постави файла под карантина, преди той да може да причини вреда.

Влияе ли сканирането в реално време на производителността на компютъра ми?

Обикновено не забелязвате процеса на сканиране, тъй като отнема малко време и системни ресурси. Колко време и системни ресурси отнема сканирането в реално време зависи например от съдържанието, местоположението и типа на файла.

Файлове, за които е необходимо повече време на сканиране:

- Файлове на преносими устройства, като CD, DVD и преносими USB устройства.
- Компресирани файлове, като *.zip* файлове.

  Бележка: Компресираните файлове не се сканират по подразбиране.

Сканирането в реално време може да забави работата на вашия компютър, ако:

- имате компютър, който не отговаря на системните изисквания или
- осъществявате достъп до много файлове едновременно. Например, когато отваряте директория, която съдържа много файлове, които трябва да бъдат сканирани.

Включване и изключване на сканирането в реално време

Оставете сканирането в реално време включено, за да спрете *злонамерения софтуер*, преди да може да навреди на компютъра ви.

Включване и изключване на сканиране в реално време:

1. На главната страница щракнете върху **Състояние**.
2. Щракнете върху **Промяна на настройките на тази страница**.

   Бележка: Нужни са ви административни права, за да изключвате функции за защита.

3. Включване и изключване на **Сканиране за вируси и шпиониращ софтуер**.
4. Щракнете върху **Затвори**.

Автоматично обработване на опасни файлове

Сканирането в реално време може да обработва опасните файлове автоматично, без да ви пита.

За да позволите на сканирането в реално време да обработва опасни файлове автоматично:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**.
3. Изберете **Автоматично обработване на опасни файлове**.

Ако решите да не обработвате опасните файлове автоматично, сканирането в реално време ви пита какво искате да правите с опасен файл при намирането му.

Обработване на шпиониращ софтуер

Сканирането за вируси и шпиониращ софтуер блокира шпиониращия софтуер веднага, когато той се опита да се се стартира.

Преди шпиониращото приложение да успее да се стартира, продуктът го блокира и ви позволява да решите какво искате да правите с него.

Изберете едно от следните действия при намиране на шпиониращ софтуер:

Действие за предприемане	Какво се случва с шпиониращия софтуер
Автоматично обработване	Позволете на продукта да избере най-доброто действие в съответствие с намерения шпиониращ софтуер.
Поставяне на шпиониращия софтуер под карантина	Преместване на шпиониращ софтуер под карантина, където той не може да навреди на компютъра ви.
Изтриване на шпиониращия софтуер	Отстраняване на всички файлове, свързани с шпиониращия софтуер, от компютъра ви.
Само блокиране на шпиониращия софтуер	Блокиране на достъпа до шпиониращия софтуер, но оставяне в компютъра.
Изключване на шпиониращия софтуер от сканирането	Позволяване на шпиониращия софтуер да се изпълнява и изключване от сканиране в бъдеще.

Обработване на рисков софтуер

Сканирането за вируси и шпиониращ софтуер блокира рисковия софтуер веднага, когато той се опита да се стартира.

Преди рисковото приложение да успее да се стартира, продуктът го блокира и ви позволява да решите какво искате да правите с него.

Изберете едно от следните действия при намиране на рисков софтуер:

Действие за предприемане	Какво се случва с рисковия софтуер
Само блокиране на рисковия софтуер	Блокиране на достъпа до рисковия софтуер, но оставяне в компютъра.
Поставяне на рисковия софтуер под карантина	Преместване на рисковия софтуер под карантина, където той не може да навреди на компютъра ви.
Изтриване на рисковия софтуер	Отстраняване на всички файлове, свързани с рисковия софтуер от компютъра ви.
Изключване на рисковия софтуер от сканиране	Позволяване на рисковия софтуер да се изпълнява и изключване от сканиране в бъдеще.

Автоматично премахване на проследяващи бисквитки

Като премахнете проследяващите бисквитки, уеб сайтовете не могат да проследяват кои сайтове в интернет посещавате.

Проследяващите бисквитки са малко файлове, които позволяват на уеб сайтовете да записват кои сайтове посещавате. Следвайте тези инструкции, за да ги премахнете от компютъра си.

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**.
3. Изберете **Премахване на проследяващи бисквитки**.
4. Щракнете върху **OK**.

Ръчно сканиране на файлове

Можете да сканирате файловете си ръчно, например когато свържете външно устройство към компютъра си, за да сте сигурни, че не съдържа злонамерен софтуер.

Стартиране на ръчно сканиране

Можете да сканирате целия компютър, да сканирате за определен тип *злонамерен софтуер* или определено местоположение.

Ако имате подозрения за определен тип *злонамерен софтуер*, можете да сканирате само за този тип. Ако имате подозрения за определено местоположение на компютъра, можете да сканирате само тази част. Тези сканирания ще свършат много по-бързо от сканиране на целия ви компютър.

За да започнете да сканирате ръчно компютъра:

1. На главната страница щракнете върху стрелката под **Сканиране**.

   Показани са опциите за сканиране.

2. Изберете типа сканиране.

   Изберете **Промяна на настройките за сканиране**, за да оптимизирате начина, по който ръчното сканиране сканира компютъра ви за вируси и други опасни приложения.

3. Ако сте избрали **Изберете какво да се сканира**, се отваря прозорец, в който можете да изберете кое местоположение да се сканира.
   Отваря се **Съветник за сканиране**.

Типове сканиране

Можете да сканирате целия компютър, да сканирате за определен тип злонамерен софтуер или определено местоположение.

Следва списък на различните типове сканиране:

Тип сканиране	Какво се сканира	Кога да използвате този тип
Сканиране за вируси и шпиониращ софтуер	Части от вашия компютър за вируси, шпиониращ софтуер и рисков софтуер	Този тип сканиране е много по-бърз от пълното сканиране. Той търси само в части от системата ви, които съдържат инсталирани програмни файлове. Този тип сканиране се препоръчва, ако искате бързо да проверите дали компютърът е чист, тъй като може да открие и премахне ефективно всякакъв активен злонамерен софтуер от компютъра ви.

Тип сканиране	Какво се сканира	Кога да използвате този тип
Пълно сканиране на компютъра	Целият ви компютър (вътрешни и външни твърди дискове) за вируси, шпиониращ софтуер и рисков софтуер	Когато искате да сте напълно сигурни, че на вашия компютър няма никакъв злонамерен или рисков софтуер. За този тип сканиране е необходимо най-много време, за да завърши. Той съчетава бързото сканиране за злонамерен софтуер и сканирането на твърдите дискове. Освен това проверява за елементи, които е възможно да са скрити от комплект за пълен достъп.
Изберете какво да се сканира	Определен файл, папка или устройство за вируси, шпиониращ софтуер и рисков софтуер	Когато имате подозрения, че е възможно на определено местоположение на вашия компютър да има злонамерен софтуер, например местоположението съдържа изтеглени файлове от потенциално опасни източници, като мрежи за споделяне на файлове с равноправен достъп. Времето за сканиране зависи от размера на целта, която сканирате. Сканирането завършва бързо, ако например сканирате папка, която съдържа само няколко малки файла.
Сканиране за комплект за пълен достъп	Важни местоположения в системата, където подозрителен елемент може да означава проблем със защитата. Сканира за скрити файлове, папки, устройства или процеси	Когато подозирате, че на компютъра ви е инсталиран комплект за пълен достъп. Ако например наскоро е бил открит злонамерен софтуер на компютъра ви и искате да се уверите, че не е инсталирал комплект за пълен достъп.

Сканиране в Windows Explorer

Можете да сканирате дискове, папки и файлове за *вируси*, *шпиониращ софтуер* и *рисков софтуер* в Windows Explorer.

За да сканирате диск, папка или файл:

1. Поставете показалеца на мишката върху диска, папката или файла, който искате да сканирате, и щракнете с десния бутон.
2. От менюто, което се показва след щракването с десния бутон, изберете **Сканирай папките за вируси** (името на опцията зависи от това дали сте избрали да сканирате диск, папка, или файл). Отваря се прозорецът на **Съветник за сканиране** и сканирането започва.

Ако бъде открит *вирус* или *шпиониращ софтуер*, **Съветник за сканиране** ви напътства в етапите на изчистване.

Избор на файлове за сканиране

Можете да изберете типовете файлове, които искате да бъдат сканирани за *вируси* и *шпиониращ софтуер* при ръчни и планирани сканирания.

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Други настройки** > **Ръчно сканиране**.
3. От **Опции за Сканиране** изберете от следните настройки:

Сканиране само на познати типове файлове	За да сканирате само тези типове файлове, които е най-вероятно да имат инфекция, например, изпълними файлове. Избирането на тази опция също така ускорява сканирането. Сканират се файловете със следните разширения: .ani, .asp, .ax, .bat, .bin, .boo, .chm, .cmd, .com, .cpl, .dll, .doc, .dot, .drv, .eml, .exe, .hlp, .hta, .htm, .html, .htt, .inf, .ini, .job, .js, .jse, .lnk, .lsp, .mdb, .mht, .mpp, .mpt, .msg, .ocx, .pdf, .php, .pif, .pot, .ppt, .rtf, .scr, .shs, .swf, .sys, .td0, .vbe, .vbs, .vxd, .wbk, .wma, .wmv, .wmf, .wsc, .wsf, .wsh, .wri, .xls, .xlt, .xml, .zip, .jar, .arj, .lzh, .tar, .tgz, .gz, .cab, .rar, .bz2 и .hqx.
Сканиране в компресирани файлове	За да сканирате архивни файлове и папки.
Използване на разширена евристика	За да използвате цялата налична евристика по време на сканиране за по-добро откриване на нов или непознат злонамерен софтуер. **Бележка:** Ако изберете тази опция, сканирането продължава повече време и може да доведе до повече грешни положителни резултати (безопасни файлове, отчетени като подозрителни).

4. Щракнете върху **OK**.

Бележка: Изключените файлове в списъка с изключения не се сканират, дори ако тук изберете да бъдат сканирани.

Какво се прави при откриване на опасни файлове

Изберете как да се обработват опасни файлове, когато бъдат открити.

За избор на действие за предприемане, когато бъде открито опасно съдържание при ръчно сканиране:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Други настройки** > **Ръчно сканиране**.
3. В**Когато се открие вирус или шпиониращ софтуер**, изберете една от следните опции:

Опция	Описание
Питай ме (по подразбиране)	Можете да изберете действие за предприемане за всеки елемент, намерен при ръчно сканиране.
Изчисти файловете	Продуктът опитва автоматично да дезинфектира инфектираните файлове, открити по време на ръчно сканиране. **Бележка:** Ако това е невъзможно, файлът се поставя под карантина (освен ако се намира на мрежов или преносим диск), така че да не може да навреди на компютъра.
Карантина на файловете	Продуктът премества всички опасни файлове, открити при ръчно сканиране, под карантина, така че да не могат да навредят на компютъра.
Изтрий файловете	Продуктът изтрива всички опасни файлове, открити при ръчно сканиране.

Опция	Описание
Само съобщаване	Продуктът оставя непроменени всички опасни файлове, открити при ръчно сканиране, и записва откриването им в отчета за сканиране. **Бележка:** Ако сканирането в реално време е изключено, злонамереният софтуер все още ще може да навреди на компютъра, ако изберете тази опция.

Бележка: Когато при автоматично сканиране са открити опасни файлове, те се изчистват автоматично.

Планиране на сканиране

Настройте компютъра си да сканира и отстранява вируси и други опасни приложения, когато не го използвате, или настройте сканирането да се изпълнява периодично, за да се уверите, че компютърът ви е чист.

За да планирате сканиране:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Други настройки** > **Планирано сканиране**.
3. Включване на **Планирано сканиране**.
4. Изберете кога искате да стартира сканирането.

Опция	Описание
Ежедневно	Сканиране на компютъра ви всеки ден.
Всяка седмица	Сканиране на компютъра ви в избрани дни от седмицата. Изберете дните от списъка.
Всеки месец	Сканиране на компютъра ви в избрани дни от месеца. За избор на дни: 1. Изберете една от опциите в **Ден**. 2. Изберете деня от месеца от списъка до избрания ден.

5. Изберете кога искате да започне сканирането в избраните дни.

Опция	Описание
Начален час	Стартиране на сканирането в посочения час.
След като компютърът не се използва за	Стартиране на сканирането, след като не сте използвали компютъра определен период от време.

Планираното сканиране използва настройките за ръчно сканиране, когато сканира компютъра ви, с тази разлика, че винаги сканира архивите и изчиства опасните файлове автоматично.

Сканиране на имейл

Сканирането на имейл ви защитава от получаването на опасни файлове с имейлите, изпратени до вас.

Сканирането за вируси и шпиониращ софтуер трябва да е включено, за да сканира имейлите за вируси.

За да включите сканиране на имейли:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**.
3. Изберете **Отстраняване на опасни прикачени файлове от съобщенията**.
4. Щракнете върху **OK**.

Кога се сканират имейл съобщенията и прикачените файлове

Сканирането за вируси и шпиониращ софтуер може да премахне опасно съдържание в имейлите, които получавате.

Сканирането за вируси и шпиониращ софтуер премахва опасни имейл приложения, получени от имейл програми, напр. Microsoft Outlook и Outlook Express, Microsoft Mail или Mozilla Thunderbird. То сканира шифрованите имейл съобщения и прикачени файлове всеки път когато вашата имейл програма ги получи от сървъра за поща чрез протокола POP3.

Сканирането за вируси и шпиониращ софтуер не може да сканира имейл съобщения в уеб имейл, които включват пощенски приложения, които се изпълняват в интернет браузъра ви като Hotmail, Yahoo! mail или Gmail. Вие все още сте защитени от *вируси*, дори да не отстраните опасните прикачени файлове или да използвате уеб имейл. Когато отваряте прикачени файлове в имейл, сканирането в реално време отстранява всички опасни файлове преди да могат да навредят.

Бележка: Сканирането в реално време защитава само вашия компютър, но не и приятелите ви. Сканирането в реално време не сканира прикачените файлове, освен ако не отворите прикачения файл. Това означава, че ако използвате уеб имейл и препратите съобщение, преди да отворите прикачения файл, е възможно да препратите инфектиран имейл на приятелите си.

Преглед на резултатите от сканирането

Хронологията за вируси и шпиониращ софтуер показва всички опасни файлове, открити от продукта.

Понякога продуктът не може да изпълни избраното действие, когато намери нещо опасно. Ако например изберете да изчистите файлове, но някой файл не може да бъде изчистен, продуктът ще го премести под карантина. Можете да прегледате тази информация в хронологията за вируси и шпиониращ софтуер.

За да прегледате хронологията:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**.
3. Щракнете върху **Преглед на хронологията на премахване**.

Хронологията за вируси и шпиониращ софтуер показва следната информация:

- дата и час на намиране на опасния файл,
- име на злонамерения софтуер и неговото местоположение на компютъра и
- изпълненото действие.

Как да се изключат файлове от сканирането

Понякога може да искате да изключите някои файлове от сканирането. Изключените елементи не се сканират, освен ако не ги отстраните от списъка за изключени елементи.

Бележка: Списъците с изключения са различни за сканиране в реално време и ръчно сканиране. Ако например изключите файл от сканирането в реално време, той ще бъде сканиран при ръчно сканиране, освен ако не го изключите и оттам.

Изключване на типове файлове

Когато изключвате файлове по тип, файловете с посочени разширения не се сканират за опасно съдържание.

За да добавите или отстраните тип файлове, които искате да изключите:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете дали искате да изключите типа файлове от сканиране в реално време или ръчно сканиране:
   - Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**, за да изключите типа файл от сканирането в реално време.
   - Изберете **Други настройки** > **Ръчно сканиране**, за да изключите типа файл от ръчното сканиране.
3. Щракнете върху **Изключване на файлове от сканирането**.
4. За да изключите тип файл:
   a) Изберете раздела **Типове файлове**.
   b) Изберете **Изключи файлове с тези разширения**.
   c) В полето до бутона **Добави** въведете разширение на файл, което показва типа файл, който искате да изключите.

      За да зададете файлове, които нямат разширение, въведете ".". Можете да използвате заместващия знак "?", за да представите произволен отделен знак, или "*", за да представите произволен брой знаци.

      За да изключите например изпълнимите файлове, въведете в полето exe.
   d) Щракнете върху **Добави**.
5. Повторете предишната стъпка за всяко друго разширение, което искате да бъде изключено от сканирането за вируси.
6. Щракнете върху **OK**, за да затворите диалоговия прозорец **Изключване от сканиране**.
7. Щракнете върху **OK**, за да приложите новите настройки.

Избраният тип файлове е изключен от бъдещо сканиране.

Изключване на файлове според местоположение

Когато изключвате файлове по местоположение, файловете в посочени папки и твърди дискове не се сканират за опасно съдържание.

За добавяне или премахване на местоположения на файлове, които искате да изключите:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете дали искате да изключите местоположението от сканиране в реално време или ръчно сканиране:
   - Изберете **Компютър** > **Сканиране за вируси и шпиониращ софтуер**, за да изключите местоположението от сканиране в реално време.
   - Изберете **Компютър** > **Ръчно сканиране**, за да изключите местоположението от ръчно сканиране.
3. Щракнете върху **Изключване на файлове от сканирането**.
4. За да изключите файл, устройство или папка:
   a) Изберете раздела **Обекти**.
   b) Изберете **Изключи обекти (файлове, папки, ...)**.
   c) Щракнете върху **Добави**.
   d) Изберете файла, устройството или папката, която желаете да изключите от сканирането за вируси.

      Бележка: Възможно е някои устройства да са преносими, например CD, DVD или мрежови устройства. Мрежовите устройства и празните преносими устройства не могат да бъдат изключени.

   e) Щракнете върху **OK**.
5. Повторете предишната стъпка, за да изключите други файлове, устройства или папки от сканирането за вируси.
6. Щракнете върху **OK**, за да затворите диалоговия прозорец **Изключване от сканиране**.
7. Щракнете върху **OK**, за да приложите новите настройки.

Избраните файлове, твърди дискове или папки са изключени от бъдещо сканиране.

Преглед на изключени приложения

Можете да прегледате приложенията, които сте изключили от сканирането, и да ги премахнете от списъка с изключения, ако искате да ги сканирате в бъдеще.

Ако сканирането в реално време или ръчното сканиране открие приложение, което се държи като шпиониращ или рисков софтуер, но за което знаете, че е безопасно, можете да го изключите от сканиране, така че продуктът да не ви предупреждава повече за него.

Бележка: Ако приложението се държи като вирус или друг злонамерен софтуер, то не може да бъде изключено.

Не можете директно да изключвате приложения. Новите приложения се показват в списъка с изключения само ако ги изключите по време на сканиране.

За да прегледате приложенията, които са изключени от сканирането:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете дали искате да прегледате приложенията, изключени от сканирането в реално време или ръчното сканиране:
   - Изберете **Компютър** > **Сканиране за вируси и шпиониращ софтуер**, за да прегледате приложенията, изключени от сканиране в реално време.
   - Изберете **Компютър** > **Ръчно сканиране**, за да прегледате приложенията, изключени от ръчно сканиране.
3. Щракнете върху **Изключване на файлове от сканирането**.

4. Изберете раздела **Приложения**.

   Бележка: Могат да бъдат изключени само приложения на шпиониращ софтуер и рисков софтуер, но не и вируси.

5. Ако искате да сканирате изключените приложения отново:
   a) Изберете приложението, което искате да включите в сканирането.
   b) Щракнете върху **Премахни**.
6. Щракнете върху **OK**, за да затворите диалоговия прозорец **Изключване от сканиране**.
7. Щракнете върху **OK**, за да излезете.

Как се използва карантината

Карантината е сигурно хранилище за файлове, които могат да бъдат опасни.

Файловете под карантина не могат да се разпространят или да причинят вреда на компютъра ви.

Продуктът може да поставя под карантина *злонамерен*, *шпиониращ* и *рисков софтуер*, за да ги обезвреди. По-късно, при необходимост можете да възстановите приложения или файлове от карантината.

Ако даден елемент, поставен под карантина, не ви е необходим, можете да го изтриете. Изтриването на елемент от карантината го премахва завинаги от компютъра ви.

- По принцип можете да изтривате поставен под карантина *злонамерен софтуер*.
- В повечето случаи можете да изтриете поставен под карантина *шпиониращ софтуер*. Възможно е поставеният под карантина *шпиониращ софтуер* да е част от легитимна софтуерна програма и премахването му да попречи на правилната работа на действителната програма. Ако искате да запазите програмата на компютъра, можете да възстановите поставения под карантина *шпиониращ софтуер*.
- Поставеният под карантина *рисков софтуер* може да е легитимна софтуерна програма. Ако сте инсталирали и настроили сами програмата, можете да я възстановите от карантината. Ако *рисковият софтуер* е инсталиран без знанието ви, най-вероятно е инсталиран с лоши намерения и трябва да бъде изтрит.

Преглед на поставените под карантина елементи

Можете да видите повече информация за елементите в карантината.

За да видите информация за елементите в карантината:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**.
3. Щракнете върху **Преглед на карантината**.
   Страницата **Карантина** показва общия брой елементи, съхранявани в карантината.
4. За да видите подробна информация за елементите в карантината, щракнете върху **По-подробно**.

   Можете да сортирате съдържанието или по име на злонамерен софтуер, или по път до файл.

   Показва се списък на първите 100 елемента с типа на поставения под карантина елемент, неговото име и пътя, където са били инсталирани файловете.
5. За да видите повече информация за елемент в карантината, щракнете върху иконата до елемента в колоната **Състояние**.

Възстановяване на поставени под карантина елементи

Можете да възстановите поставени под карантина елементи, които са ви необходими.

Можете да възстановите приложения или файлове от карантината, ако са ви необходими. Не възстановявайте никакви елементи от карантината освен ако не сте сигурни, че не представляват никаква заплаха. Възстановените елементи се връщат в първоначалното местоположение във вашия компютър.

За да възстановите поставени под карантина елементи:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **Сканиране за вируси и шпиониращ софтуер**.
3. Щракнете върху **Преглед на карантината**.
4. Изберете поставените под карантина елементи, които искате да възстановите.
5. Щракнете върху **Възстанови**.

Какво представлява DeepGuard

DeepGuard анализира съдържанието на файловете и поведението на приложенията и следи приложенията, които не са надеждни.

DeepGuard блокира нови и неоткрити *вируси*, *червеи* и други опасни приложения, които се опитват да извършват промени в компютъра ви, и блокира достъпа на подозрителни приложения до интернет.

Когато DeepGuard идентифицира ново приложение, което се опитва да направи потенциално опасни промени в системата, позволява на приложението да се изпълни в безопасна зона. В безопасната зона приложението не може да навреди на компютъра ви. DeepGuard анализира какви промени е опитало да направи приложението и въз основа на това решава колко вероятно е то да е *злонамерен софтуер*. Ако е вероятно приложението да е *злонамерен софтуер*, DeepGuard го блокира.

Потенциално опасните системни промени на системата, които DeepGuard идентифицира, включват:

- промени в системните настройки (системния регистър на Windows);
- опити за изключване на важни системни програми, например програми за защита като този продукт, и
- опити за редактиране на важни системни файлове.

Включване и изключване на DeepGuard

Оставете DeepGuard включен, за да не позволите на подозрителни приложения да правят потенциално опасни промени в системата на компютъра ви.

Ако имате Windows XP, уверете се, че сте инсталирали Service Pack 2, преди да включите DeepGuard.

Включване и изключване на DeepGuard:

1. На главната страница щракнете върху **Състояние**.
2. Щракнете върху **Промяна на настройките на тази страница**.

   Бележка: Нужни са ви административни права, за да изключвате функции за защита.

3. Включване и изключване на **DeepGuard**.
4. Щракнете върху **Затвори**.

Позволяване на приложения, блокирани от DeepGuard

Можете да контролирате кои приложения се позволяват и блокират от DeepGuard.

Понякога е възможно DeepGuard да блокира безопасно приложение, дори когато искате да го използвате и знаете, че е не е вредно. Това се случва, понеже приложението опитва да направи промени в системата, които може да са потенциално опасни. Възможно е без да искате, да сте блокирали приложението, когато се е показал изскачащ прозорец на DeepGuard.

За позволяване на приложение, блокирано от DeepGuard:

1. На главната страница щракнете върху **Инструменти**.
2. Щракнете върху **Приложения**.
   Показва се списък **Наблюдавани приложения**.
3. Намерете приложението, което искате да позволите.

   Бележка: Можете да щракнете върху заглавията на колоните, за да сортирате списъка. Щракнете например върху колоната **Разрешение**, за да подредите списъка в групи от позволени и забранени програми.

4. Изберете **Позволи** в колоната **Разрешение**.
5. Щракнете върху **Затвори**.

DeepGuard позволява на приложението отново да прави промени в системата.

Използване на DeepGuard в режим на съвместимост

За максимална защита DeepGuard временно модифицира изпълняващите се програми. Някои програми проверяват дали не са повредени или променени и може да са несъвместими с тази функция. Например онлайн игрите с инструменти против измами проверяват дали са били модифицирани по някакъв начин, когато се изпълняват. В тези случаи можете да включите режима на съвместимост.

Включване на режима на съвместимост:

1. На главната страница щракнете върху **Настройки**.

   Бележка: За да промените настройките са нужни права на администратор.

2. Изберете **Защита на компютъра** > **DeepGuard**.
3. Изберете **Използване на режим на съвместимост**.
4. Щракнете върху **OK**.

Какво да правите с предупреждения за подозрително поведение

DeepGuard следи приложения, които не са надеждни. Ако следено приложение се опита да получи достъп до интернет, да направи промени в системата ви или се държи подозрително, DeepGuard го блокира.

Когато изберете **Предупреди ме за подозрително поведение** в настройките на DeepGuard, функцията ви известява, когато открие потенциално опасно приложение или когато стартирате приложение с неизвестна репутация.

За да решите какво искате да правите с приложението, блокирано от DeepGuard:

1. Щракнете върху **Детайли**, за да видите повече информация за програмата.
   Секцията с детайли ви показва:

   - местоположението на приложението,
   - репутацията на приложението в мрежата за защита в реално време и

- колко често използвано е приложението.

2. Решете дали можете да се доверите на блокираното от DeepGuard приложение:

- Изберете **Мога да се доверя на приложението. Нека продължи.**, ако не искате го блокирате.

  По-вероятно е приложението да е безопасно, ако:

  - DeepGuard го е блокирал в резултат на нещо, което вие сте направили,
  - разпознавате приложението или
  - сте го получили от доверен източник.

- Изберете **Не мога да се доверя на приложението. Продължи блокирането.**, ако искате то да остане блокирано.

  По-вероятно е приложението да е опасно, ако:

  - не е често използвано,
  - репутацията му е неизвестна или
  - не го разпознавате.

3. Ако искате да изпратите подозрително приложение за анализ:

a) Щракнете върху **Докладване на приложението на F-Secure**.
Продуктът показва условията за изпращане.

b) Щракнете върху **Приемам**, ако сте съгласни с условията и искате да изпратите примера.

Препоръчваме ви да изпратите пример, когато:

- DeepGuard блокира приложение, за което знаете, че е безопасно или
- подозирате, че приложението може да е *злонамерен софтуер*.