F-Secure Anti-Virus 2013

Vsebina

Poglavje 1: Namestitev.....5

Pred prvo namestitvijo.....6
Prva namestitev izdelka.....6
Namestitev in posodobitev programov.....6
Pomoč in podpora.....7

Poglavje 2: Uvod.....9

Kako uporabiti samodejne posodobitve.....10
Preverjanje stanja posodobitev.....10
Spreminjanje nastavitev internetne povezave.....10
Preverite stanje omrežja s sprotno zaščito.....11
Kako videti, kaj je naredil izdelek.....11
Prikaz zgodovine obvestil.....11
Spreminjanje nastavitev obvestil.....11
Real-time Protection Network.....12
Kaj je Real-time Protection Network.....12
Prednosti storitve Real-time Protection Network.....12
Podatki, ki jih lahko posredujete.....13
Naša zaščita vaše zasebnosti.....14
Postanite sodelavec v storitvi Real-time Protection Network.....14
Vprašanja o storitvi Real-time Protection Network.....14
Kako vem, ali je moja naročnina veljavna.....15
Središče za dejanja.....15
Aktiviranje naročnine.....15

Poglavje 3: Uvod.....17

Ogled skupnega stanja zaščite.....18
Prikaz statistike izdelka.....18
Obdelava posodobitev izdelka.....19
Prikaz različic zbirke podatkov.....19
Spreminjanje nastavitev mobilne širokopasovne povezave.....19
Virusi in druga zlonamerna programska oprema.....20
Virusi.....20
Vohunski programi.....20
Korenski kompleti.....21
Tvegana programska oprema.....21

Poglavje 4: Varovanje računalnika pred zlonamerno programsko opremo.23
Pregled računalnika....24
Samodejno pregledovanje datotek....24
Ročno pregledovanje datotek....26
Preglej e-pošto....29
Prikaz rezultatov pregleda....29
Kako izključiti datoteke iz pregleda....30
Izvzemanje vrst datotek....30
Izvzemanje datotek glede na mesto....31
Ogled izvzetih programov....31
Uporaba karantene....32
Ogled elementov v karanteni....32
Obnavljanje elementov v karanteni....33
Kaj je DeepGuard?....33
Vklop ali izklop programa DeepGuard....33
Dovoli programe, ki jih tehnologija DeepGuard preprečuje....34
Uporabi DeepGuard v združljivostnem načinu....34
Kako obravnavati opozorila o sumljivem delovanju....34

Poglavje

1

Namestitev

Teme:

- *Pred prvo namestitvijo*
- *Prva namestitev izdelka*
- *Namestitev in posodobitev programov*
- *Pomoč in podpora*

Pred prvo namestitvijo

Zahvaljujemo se vam, ker ste izbrali F-Secure.

Za namestitev izdelka potrebujete:

- Namestitveni CD ali paket. Če uporabljate miniprenosnik brez pogona CD, lahko namestitveni paket prenesete s spletnega mesta *www.f-secure.com/netbook*.
- Vaš naročniški ključ.
- Internetno povezavo.

Če imate varnostni izdelek drugega prodajalca, ga bo namestitveni program poskusil samodejno odstraniti. Če se to ne zgodi, ga odsranite ročno.

Opomba: Če imate v računalniku več računov, se pri namestitvi prijavite z računom, ki ima skrbniške pravice.

Prva namestitev izdelka

Navodila za namestitev izdelka

Izdelek namestite po spodnjih navodilih:

1. Vstavite CD ali dvokliknite preneseni namestitveni program.

   Če se CD ne zažene samodejno, odprite Windows Explorer, dvokliknite ikono pogona CD-ROM in nato še namestitveno datoteko, da začnete namestitev.

2. Sledite navodilom na zaslonu.

   - Če ste kupili izdelek na CD-ju v trgovini, je naročniški ključ na ovitku priročnika za hitro namestitev.
   - Če ste izdelek prenesli z e-trgovine F-Secure eStore, je naročniški ključ v e-poštnem sporočilu s potrditvijo nakupa.

   Računalnik boste morda morali znova zagnati pred preverjanjem veljavnosti naročnine in prenosom najnovejših posodobitev s spleta. Če izvajate namestitev s CD-ja, pred vnovičnim zagonom računalnika ne pozabite odstraniti namestitvenega CD-ja.

Namestitev in posodobitev programov

Navodila za aktivacijo nove naročnine.

Sledite tem navodilom za aktivacijo nove naročnine ali namestitev novega programa v podoknu za zagon:

Opomba: Ikona podokna za zagon je v sistemski vrstici sistema Windows.

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Potrdite **Ogled mojih naročnin**
3. V razdelku **Moje naročnine** odprite stran **Stanje naročnine** in kliknite **Aktivna naročnina**.
   Odpre se okno **Aktivna naročnina**.
4. Vnesite naročniški ključ za program in kliknite **V redu**.

5. Ko je veljavnost naročnine preverjena in naročnina aktivirana, kliknite **Zapri**.
6. V razdelku **Moje naročnine** odprite stran **Stanje namestitve**. Če se namestitev ne zažene samodejno, sledite tem navodilom:
   a) Kliknite **Namesti**.
      Odpre se okno za namestitev.
   b) Kliknite **Naprej**.
      Program je prenesen in namestitev se začne.
   c) Po dokončani namestitvi klikinite **Zapri**.

Aktivirana je nova naročnina.

Pomoč in podpora

Spletno pomoč za izdelek odprete tako, da kliknete ikono za pomoč oziroma tako, da na poljubnem zaslonu izdelka pritisnete tipko F1.

Ko registrirate licenco, boste upravičeni do dodatnih storitev, kot so brezplačne posodobitve izdelkov in podpora za izdelek. Licenco lahko registrirate na spletnem mestu *www.f-secure.com/register*.

Poglavje

2

Uvod

Teme:

- *Kako uporabiti samodejne posodobitve*
- *Kako videti, kaj je naredil izdelek*
- *Real-time Protection Network*
- *Kako vem, ali je moja naročnina veljavna.*

Informacije o uvodu v izdelek.

V tem razdelku je opisano, kako spremenite pogoste nastavitve in upravljate naročnine prek podokna za zagon.

Pogoste nastavitve podokna za zagon so nastavitve, ki veljajo za vse programe, nameščene v podoknu za zagon. Namesto da bi spreminjali nastavitve ločeno v vsakem programu, lahko preprosto uredite pogoste nastavitve, ki jih nato uporabite v vseh nameščenih programih.

Pogoste nastavitve podokna za zagon vključujejo:

- Prenose, kjer so prikazane informacije o prenesenih posodobitvah in ročno preverite, ali so na voljo nove posodobitve.
- Nastavitve povezave, kjer lahko spremenite način vzpostavitve povezave računalnika z internetom.
- Obvestila, kjer si lahko ogledate pretekla obvestila in nastavite obvestila, ki jih želite prikazati.
- Nastavitve zasebnosti, kjer lahko računalniku dovolite vzpostavitev povezave z omrežjem, ki omogoča sprotno zaščito, ali ne.

Tudi v podoknu za zagon lahko upravljate svoje naročnine za nameščene programe.

Kako uporabiti samodejne posodobitve

Samodejne posodobitve skrbijo za redno posodabljanje zaščite računalnika.

Izdelek v računalnik prenese najnovejše posodobitve, kadar ste povezani z internetom. Zaznava omrežni promet in ne moti uporabe interneta, tudi če imate počasno omrežno povezavo.

Preverjanje stanja posodobitev

Oglejte si datum in uro zadnje posodobitve.

Če je samodejno posodabljanje vklopljeno, izdelek samodejo prejema zadnje posodobitve, kadar je vzpostavljena povezava z internetom.

Če se želite prepričati, da imate najnovejše posodobitve:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Odpri pogoste nastavitve**.
3. Izberite **Samodejne posodobitve** > **Prenosi**.
4. Kliknite **Preveri zdaj**.
   Izdelek vzpostavi povezavo z internetom in preveri, ali so na voljo najnovejše posodobitve. Če zaščita ni posodobljena, prenese najnovejše posodobitve.

   Opomba: Če uporabljate modem oziroma internetno povezavo ISDN, mora biti povezava vzpostavljena, če želite preveriti, ali so na voljo posodobitve.

Spreminjanje nastavitev internetne povezave

Po navadi ni treba spreminjati privzetih nastavitev, vendar lahko konfigurirate način povezave strežnika z internetom tako, da samodejno prejemate posodobitve.

Če želite spremeniti nastavitve internetne povezave:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Odpri pogoste nastavitve**.
3. Izberite **Samodejne posodobitve** > **Povezava**.
4. Na seznamu **Internetna povezava**, kako je računalnik povezan z internetom.
   - Izberite **Domnevaj nepretrgano povezavo**, če imate neprekinjeno omrežno povezavo.

     Opomba: Če računalnik nima nepretrgane omrežne povezave, temveč klicno povezavo, ki jo morate vsakič znova vzpostaviti, se utegne zgoditi, da bo večkrat skušal vzpostaviti povezavo, če potrdite možnost **Domnevaj nepretrgano povezavo**.
   - Možnost **Zaznaj povezavo** izberite, če želite, da program prenese posodobitve samo, kadar zazna dejavno omrežno povezavo.
   - Možnost **Zaznaj promet** izberite, če želite, da program posodobitve prenese samo, kadar zazna še drug omrežni promet.

     Namig: Če imate neobičajno strojno konfiguracijo, zaradi katere program takrat, ko je izbrana možnost **Zaznaj povezavo**, zazna dejavno omrežno povezavo, čeprav te ni, izberite možnost **Zaznaj promet**.

5. Na seznamu **Strežnik proxy za HTTP** izberite, ali naj računalnik za povezavo z internetom uporablja *strežnik proxy* ali ne.
   - Možnost **Brez strežnika proxy za HTTP** izberite, ali je računalnik z internetom povezan neposredno.
   - Možnost **Ročno konfiguriraj namestniški strežnik za HTTP** izberite, če želite nastavitve za *namestniški strežnik za HTTP* določiti ročno.
   - Izberite **Uporabi brskalnikov proxy za HTTP**, da uporabite iste nastavitve *proxyja za HTTP*, s katerimi ste konfigurirali svoj spletni brskalnik.

Preverite stanje omrežja s sprotno zaščito

Pravilno delovanje je pri številnih funkcijah izdelkov odvisno od povezljivosti omrežja s sprotno zaščito.

Če pride do težav z omrežjem ali požarni zid blokira promet v omrežju s sprotno zaščito, je stanje »Povezava je bila prekinjena«. Če ni nameščen noben izdelek, za katerega potrebujete dostop do omrežja s sprotno zaščito, je stanje »Ni v uporabi«.

Preverjanje stanja:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Odpri pogoste nastavitve**.
3. Izberite **Samodejne posodobitve** > **Povezava**.

V odseku »**Omrežje s sprotno zaščito**« je prikazano trenutno stanje omrežja s sprotno zaščito.

Kako videti, kaj je naredil izdelek

Na strani za **Obvestila** vidite, s katerimi dejanji je izdelek zaščitil vaš računalnik.

Izdelek ob izvedbi dejanja prikaže obvestilo, ko na primer najde virus, ki ga blokira. Nekatera obvestila lahko pošlje tudi vaš ponudnik storitve, da vas na primer obvesti o novih storitvah, ki so na voljo.

Prikaz zgodovine obvestil

V zgodovini obvestil vidite, katera obvestila so bila prikazana

Če želite prikazati zgodovino obvestil:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Odpri pogoste nastavitve**.
3. Izberite **Drugo** > **Obvestila**.
4. Kliknite **Prikaži zgodovino obvestil**.
   Odpre se seznam zgodovine obvestil.

Spreminjanje nastavitev obvestil

Izberete lahko vrste obvestil, ki naj jih izdelek prikaže.

Če želite spremeniti nastavitve obvestil:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Odpri pogoste nastavitve**.

3. Izberite **Drugo** > **Obvestila**.
4. Potrdite ali počistite možnost **Dovoli programska sporočila**, da vklopite ali izklopite prejemanje programskih sporočil.

   Če je nastavitev vklopljena, izdelek prikaže obvestila iz nameščenih programov.
5. Potrdite ali počistite možnost **Dovoli promocijska sporočila**, da vklopite ali izklopite prejemanje promocijskih sporočil.
6. Kliknite **V redu**.

Real-time Protection Network

V tem dokumentu je opisana storitev Real-time Protection Network, spletna storitev družbe F-Secure, ki omogoča prepoznavanje čistih programov in spletnih mest, pri čemer zagotavlja zaščito pred zlonamerno programsko opremo in zlorabami spletnih mest.

Kaj je Real-time Protection Network

Real-time Protection Network je spletna storitev, ki omogoča hiter odziv na najnovejše internetne grožnje.

Kot sodelavec v storitvi Real-time Protection Network nam pomagate povečati zaščito pred novimi in prihajajočimi grožnjami. Storitev Real-time Protection Network omogoča zbiranje statističnih podatkov o določenih neznanih, zlonamernih ali sumljivih programih in o tem, kako lahko ogrozijo vaš računalnik. Ti podatki so anonimni in posredovani družbi F-Secure za potrebe analize kombiniranih podatkov. Analizirane podatke uporabimo za izboljšave zaščite vašega računalnika pred najnovejšimi grožnjami in zlonamernimi datotekami.

Delovanje storitve Real-time Protection Network

Kot sodelavec v storitvi Real-time Protection Network nam lahko posredujete informacije o neznanih programih in spletnih mestih ter o zlonamernih in izkoriščevalskih programih na spletnih mestih. Real-time Protection Network ne omogoča sledenja vašim spletnim dejavnostim ali zbiranja informacij o spletnih mestih, ki so že bila analizirana, prav tako ne omogoča zbiranja informacij o čistih programih, ki so nameščeni v vaš računalnik.

Če ne želite prispevati teh podatkov, storitev Real-time Protection Network ne bo zbirala informacij o nameščenih programih ali obiskanih spletnih mestih. Kljub temu mora izdelek v strežnikih F-Secure izvesti poizvedbo o slovesu programov, spletnih mest, sporočil in drugih predmetov. Poizvedbo izvede z uporabo kriptografske kontrolne vsote, s katero sam predmet poizvedbe ne pošlje družbi F-Secure. Družba F-Secure ne sledi podatkom po uporabnikih; poveča se le številka na števcu zadetkov za datoteke oz. spletna mesta.

Vsega prometa v storitvi Real-time Protection Network ni mogoče povsem zaustaviti, saj je sestavni del zaščite, ki jo ponuja izdelek.

Prednosti storitve Real-time Protection Network

S storitvijo Real-time Protection Network dobite hitrejšo in bolj natančno opredeljeno zaščito pred najnovejšimi grožnjami, pri čemer ne boste prejemali nepotrebnih opozoril o sumljivih programih, ki niso zlonamerni.

Kot sodelavec v storitvi Real-time Protection Network nam lahko pomagate najti novo in nezaznano zlonamerno programsko opremo ter iz naše zbirke definicij virusov odstraniti morebitne napačne pozitivne prepoznave.

Vsi sodelavci v storitvi Real-time Protection Network si med seboj pomagajo. Kadar storitev Real-time Protection Network najde sumljiv program v vašem računalniku, lahko izkoristite prednost rezultatov analize, če je bil isti program že najden v nekem drugem računalniku. Real-time Protection Network omogoča izboljšanje skupne učinkovitosti delovanja vašega računalnika, saj nameščenemu varnostnemu izdelku ni treba znova pregledati programov, ki jih je analizirala storitev Real-time Protection Network in odkrila, da so čisti. Podobno je prek storitve Real-time Protection Network omogočena skupna raba podatkov o zlonamernih spletnih

mestih in neželenih množičnih sporočilih, tako da vam lahko zagotovimo bolj natančno opredeljeno zaščito pred zlorabami spletnih mest in sporočili neželene pošte.

Več kot je ljudi, ki sodelujejo v storitvi Real-time Protection Network, bolje so zaščiteni posamezni sodelavci.

Podatki, ki jih lahko posredujete

Kot sodelavec v storitvi Real-time Protection Network nam posredujete informacije o programih, shranjenih v računalniku, in spletnih mestih, ki jih obiskujete, tako da lahko Real-time Protection Network zagotovi zaščito pred najnovejšimi zlonamernimi programi in sumljivimi spletnimi mesti.

Analiza slovesa

Real-time Protection Network zbira informacije le o programih, ki niso znani, in o datotekah, ki so sumljive ali za katere se ve, da so zlonamerne.

Real-time Protection Network zbira anonimne informacije o čistih in sumljivih programih v vašem računalniku. Real-time Protection Network zbira le informacije o izvedljivih datotekah (kot so npr. datoteke v obliki zapisa Portable Executable v sistemu Windows z datotečnimi priponami .cpl, .exe, .dll, .ocx, .sys, .scr in .drv).

Zbrane informacije vključujejo:

- pot datoteke do mesta programa v računalniku,
- velikost datoteke in čas ustvarjanja ali spreminjanja,
- atributi datotek in pravice,
- informacije o podpisu datoteke,
- trenutna različica datoteke in podjetje, ki jo je ustvarilo,
- izvor dokumenta ali spletni naslov zanj in
- Rezultati analize programa F-Secure DeepGuard in protvirusnega programa pregledanih datotek in
- druge podobne informacije.

Real-time Protection Network nikoli ne zbira nobenih informacij o osebnih dokumentih, razen če ni bilo odkrito, da so okuženi. Za vse vrste zlonamernih datotek zbere ime okužbe in podatek o stanju čiščenja datoteke.

Storitev Real-time Protection Network omogoča tudi pošiljanje sumljivih programov v analizo. Pošljete lahko le programe v obliki zapisa datotek Portable Executable. Real-time Protection Network nikoli ne zbira nobenih podatkov o zasebnih dokumentih, ki tudi niso nikoli samodejno preneseni v analizo.

Pošiljanje datotek za analizo

Storitev Real-time Protection Network omogoča tudi pošiljanje sumljivih programov v analizo.

Posamezne sumljive programe lahko pošljete ročno, ko vas izdelek pozove. Pošljete lahko le datoteke v obliki zapisa Portable Executable. Storitev Real-time Protection Network nikoli ne prenese vaših osebnih dokumentov.

Analiza slovesa spletnega mesta

Real-time Protection Network ne sledi vašim spletnim aktivnostim niti ne zbira informacij o spletnih mestih, ki so že bila analizirana. Medtem ko brskate po spletu preveri, ali so obiskana spletna mesta varna. Ko obiščete spletno mesto, Real-time Protection Network preveri, ali je varno in vas obvesti, če je mesto ocenjeno kot sumljivo ali škodljivo.

Če je na obiskanem spletnem mestu zlonamerna ali sumljiva vsebina ali znan izkoriščevalski program, Real-time Protection Network zbere vse podatke o spletnem naslovu mesta, tako omogoči analizo vsebine spletne strani.

Če obiščete spletno mesto, ki še ni bilo ocenjeno, Real-time Protection Network zbere podatke o imenu domene in poddomene, in v nekaterih primerih o poti do strani, ki ste jo obiskali, tako da je mogoče mesto oceniti in analizirati. Vsi parametri spletnega naslova, ki morda vsebujejo informacije, ki jih je mogoče povezati z vami v obliki, ki dopušča identifikacijo posameznika, so odstranjeni zaradi zaščite vaše zasebnosti.

Opomba: Real-time Protection Network ne ocenjuje ali analizira spletnih mest v zasebnih omrežjih, zato nikoli ne zbira nobenih podatkov o naslovih IP zasebnih omrežij (na primer intranetih v podjetjih).

Analiza sistemskih podatkov

Real-time Protection Network zbira podatke o imenu in različici operacijskega sistema, podatke o internetni povezavi in statistične podatke o uporabi storitve Real-time Protection Network (na primer število poizvedb glede slovesa spletnega mesta in povprečno število vrnjenih rezultatov za poizvedbe), kar nam omogoča, da spremljamo in izboljšujemo storitev.

Naša zaščita vaše zasebnosti

Informacije prenašamo varno, pri čemer so samodejno odstranjeni vsi morebitni vsebovani osebni podatki.

Real-time Protection Network odstrani podatke, ki omogočajo identifikacijo posameznika, preden so posredovani družbi F-Secure, in med prenosom šifrira vse zbrane podatke, da jih zaščiti pred nepooblaščenim dostopom. Zbranih informacij ne obdela posamezno, temveč jih združi z informacijami od drugih sodelavcev v storitvi Real-time Protection Network. Vse podatke statistično in anonimno analiziramo, kar pomeni, da nobenega podatka ne bo mogoče na noben način povezati z vami.

Med zbranimi podatki ni nobene informacije, ki omogoča identifikacijo posameznika. Real-time Protection Network ne zbira podatkov o zasebnih naslovih IP ali zasebnih podatkov, kot so e-poštni naslov, uporabniško ime in geslo. Čeprav se izredno močno trudimo, da odstranimo vse podatke, ki omogočajo identifikacijo posameznika, se lahko zgodi, da med zbranimi informacijami ostane kateri od teh podatkov. V takšnih primerih ne bomo namerno uporabili takšnih nenamerno zbranih podatkov za vašo identifikacijo.

Pri prenašanju, shranjevanju in obdelavi zbranih informacij, jih zaščitimo s strogimi varnostnimi ukrepi, ki vključuje tudi fizično, administrativno in tehnično varnostno zaščito. Informacije so shranjene na varnih mestih in v strežnikih, ki jih nadziramo, ne glede na to, ali so v naših pisarnah ali v pisarnah naših podpogodbenikov. Dostop do zbranih informacij ima le pooblaščeno osebje.

F-Secure lahko omogoči skupno rabo zbranih podatkov s svojimi podružnicami, podpogodbeniki, distributerji in partnerji, vendar to vedno naredi na način, ki ne omogoča identifikacije posameznika in v anonimni obliki.

Postanite sodelavec v storitvi Real-time Protection Network

Storitev Real-time Protection Network nam lahko pomagate izboljšati, tako da nam posredujete informacije o zlonamernih programih in spletnih mestih.

Med namestitvijo se lahko odločite, ali boste sodelovali v storitvi Real-time Protection Network. S privzetimi nastavitvami namestitve prispevate podatke v storitev Real-time Protection Network. Pozneje lahko to nastavitev v izdelku spremenite.

Sledite tem navodilom, če želite spremeniti nastavitve Real-time Protection Network:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Odpri pogoste nastavitve**.
3. Izberite**Drugo** > **Zasebnost**.
4. Če želite postati sodelavec v storitvi Real-time Protection Network, potrdite polje sodelovanja.

Vprašanja o storitvi Real-time Protection Network

Podatki za stik za kakršna koli vprašanja o storitvi Real-time Protection Network.

Če imate še kakšno vprašanje o storitvi Real-time Protection Network, se obrnite na:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finska

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

Najnovejša različica tega pravilnika je vedno na voljo na našem spletnem mestu.

Kako vem, ali je moja naročnina veljavna.

Vrsta vaše naročnine in stanje sta prikazana na strani **Stanje naročnine**.

Če bo naročnina kmalu potekla ali če je že potekla, se stanje zaščite programa v ustrezni ikoni podokna za zagon spremeni.

Veljavnost naročnine preverite tako:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Ogled mojih naročnin**.
3. Izberite **Stanje naročnin**, da prikažete informacije o naročninah za nameščene programe.
4. Izberite **Stanje namestitve**, da si ogledate, kateri programi so na voljo za namestitev.

Stanje naročnine in datum poteka sta prikazana tudi na strani **Statistika** programa. Če je vaša naročnina potekla, morate naročnino obnoviti, če želite še naprej prejemati posodobitve in uporabljati izdelek.

Opomba: Ko naročnina poteče, ikona stanja izdelka utripa v sistemski vrstici.

Središče za dejanja

V središču za dejanja so prikazane vsa pomembna obvestila, ki zahtevajo vašo pozornost.

Če je vaša naročnina potekla ali bo kmalu potekla, vas o tem obvesti središče za dejanja. Barva ozadja in vsebina sporočila središča za dejanja sta odvisna od vrste naročnine in stanja:

- Če bo vaša naročnina kmalu potekla in so na voljo brezplačne naročnine, ima sporočilo belo ozadje in gumb **Aktiviraj**.
- Če bo vaša naročnina kmalu potekla in ni na voljo brezplačnih naročnin, ima sporočilo rumeno ozadje ter gumba **Nakup** in **Vnos ključa**. Če ste že kupili novo naročnino, kliknite **Vnos ključa**, navedite naročniški ključ in aktivirajte novo naročnino.
- Če je vaša naročnina potekla in so na voljo brezplačne naročnine, ima sporočilo rdeče ozadje in gumb **Aktiviraj**.
- Če je vaša naročnina potekla in ni na voljo brezplačnih naročnin, ima sporočilo rdeče ozadje ter gumba **Nakup** in **Vnos ključa**. Če ste že kupili novo naročnino, kliknite **Vnos ključa**, navedite naročniški ključ in aktivirajte novo naročnino.

Opomba: Če kliknete povezavo **Prikaži zgodovino obvestil** v središču za dejanja, se prikaže seznam sporočil o obvestilih izdelka, ne pa tudi starejša sporočila središča za dejanja.

Aktiviranje naročnine

Ko imate novi ključ naročnine ali kodo akcije izdelka, ga morate aktivirati.

Naročnino aktivirate tako:

1. V zagonski vrstici z desno tipko miške kliknite ikono skrajno desno.
   Prikaže se pojavni meni.
2. Izberite **Ogled mojih naročnin**.
3. Izberite nekaj od tega:
   - Kliknite **Aktiviraj naročnino**.
   - Kliknite **Aktiviraj kodo akcije**.
4. V pogovornem oknu, ki se odpre, vnesite ključ nove naročnine ali kodo akcije in kliknite **V redu**.

   Namig: Če ste naročniški ključ prejeli po e-pošti, ga kopirajte iz e-poštnega sporočila in prilepite v polje.

Ko vnesete novi ključ naročnine, se na strani **Stanje naročnine** prikaže datum veljavnosti nove naročnine.

Poglavje
3

Uvod

Teme:

- *Ogled skupnega stanja zaščite*
- *Prikaz statistike izdelka*
- *Obdelava posodobitev izdelka*
- *Virusi in druga zlonamerna programska oprema*

Izdelek računalnik ščiti pred virusi in drugimi škodljivimi programi.

Izdelek pregleduje datoteke, analizira programe in se samodejno posodablja, zato vam ni treba ukrepati.

Ogled skupnega stanja zaščite

Na strani **Stanje** imate na voljo hiter pregled nameščenih funkcij izdelka in njihovega trenutnega stanja.

Stran **Stanje** odprete tako:

Na glavni strani kliknite **Stanje**.

Stran **Stanje** se odpre.

Ikone prikazujejo stanje programa in njegove varnostne funkcije.

Ikona stanja	Ime stanja	Opis
	V redu	Računalnik je zaščiten. Funkcija je vklopljena in deluje pravilno.
	Informacije	Izdelek vas seznani s posebnim stanjem funkcije. Na primer, funkcija se posodablja.
	Opozorilo	Računalnik ni povsem zaščiten. Na primer, izdelek že dlje časa ni bil posodobljen ali pa stanje funkcije zahteva vašo pozornost.
	Napaka	Vaš računalnik ni zaščiten. Na primer, vaša naročnina je potekla ali pa je pomembna funkcija izklopljena.
	Izklopljeno	Nepomembna funkcija je izklopljena.

Prikaz statistike izdelka

Na strani **Statistika** si lahko ogledate, kaj je izdelek naredil od namestitve.

Če želite odpreti stran **Statistika**:

Na glavni strani klikknite **Statistika**.

Odpre se stran **Statistika**.

- V razdelku **Zadnja uspešna posodobitev** je prikazan datum zadnje posodobitve.
- V razdelku **Iskanje virusov in vohunske programske opreme** je prikazano število datotek, ki jih je program pregledal in odstranil, odkar ste ga namestili.

- V razdelku **Programi** je prikazano, koliko programov je tehnologija DeepGuard dovolila ali blokirala od namestitve.
- V razdelku **Povezave omrežnega zidu** je prikazano število dovoljenih in blokiranih povezav od namestitve.
- V razdelku **Filtriranje neželene in lažne pošte** je prikazano število veljavnih in vsiljenih e-poštnih sporočil, ki jih je izdelek zaznal.

Obdelava posodobitev izdelka

Izdelek omogoča samodejno posodabljanje zaščite.

Prikaz različic zbirke podatkov

Na strani **Posodobitve zbirke podatkov** si lahko ogledate najnovejše čase posodobitev in številke različic.

Stran **Posodobitve zbirke podatkov** odprete tako:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Druge nastavitve** > **Različice zbirke podatkov**.

Stran **Različice zbirke podatkov** prikazuje najnovejši datum posodobitev definicij virusov in vohunskih programov, DeepGuarda ter filtriranja neželene in lažne pošte ter njihove številke različic.

Spreminjanje nastavitev mobilne širokopasovne povezave

Izberite, ali želite pri uporabi mobilnega širokopasovnega omrežja omogočiti prenos varnostnih posodobitev.

Opomba: Ta funkcija je na voljo le v sistemu Microsoft Windows 7.

Privzeto se varnostne posodobitve vedno prenesejo, kadar ste v omrežju domačega operaterja. Vendar je prenos posodobitev začasno prekinjen, kadar ste v omrežju drugega operaterja. To je zato, ker se cene povezav lahko razlikujejo od operaterja do operaterja, na primer, v različnih državah. Priporočamo vam, da teh nastavitev ne spreminjate, če želite ohraniti pasovno širino in morda tudi prihraniti stroške, ko ste v drugem omrežju.

Opomba: Ta nastavitev velja le za mobilna širokopasovna omrežja. Ko je vzpostavljena povezava med računalnikom in stacionarnim ali brezžičnim omrežjem, je omogočeno samodejno posodabljanje izdelka.

Spreminjanje nastavitve:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Druge nastavitve** > **Mobilna širokopasovna povezava** > **Prenesi varnostn e posodobitve**.
3. Izberite želene možnosti posodobitev za mobilne povezave:
   - **Samo v omrežju domačega operaterja**

     Posodobitve se vedno prenesejo v omrežju domačega operaterja. Ko ste v omrežju drugega operaterja, se prenos posodobitev začasno prekine. Priporočamo vam, da izberete to možnost, če želite ohraniti posodabljanje varnostnega izdelka ob pričakovanih stroških.
   - **Nikoli**

     Posodobitve ne bodo prenesene, kadar uporabljate mobilno širokopasovno povezavo.
   - **Vedno**

Posodobitve se vedno prenesejo, ne glede na to, v katerem omrežju ste. Izberite to možnost, če želite omogočiti posodabljanje varnosti vašega računalnika, ne glede na stroške.

4. Če se želite odločiti vsakič posebej, ko prekinete povezavo z omrežjem domačega operaterja,izberite **Vprašaj me vsakič, ko prekinem povezavo z omrežjem mojega domačega operaterja**.

Začasno prekinjene varnostne posodobitve

Varnostne posodobitve so morda začasno prekinjene, kadar uporabljate mobilno širokopasovno omrežje zunaj omrežja domačega operaterja.

V tem primeru lahko v spodnjem desnem kotu zaslona vidite obvestilo **Začasno prekinjeno**. Prenos posodobitev je začasno prekinjen, ker se cene povezav morda razlikujejo od operaterja do operaterja, na primer v različnih državah. Priporočamo vam, da teh nastavitev ne spreminjate, če želite ohraniti pasovno širino in morda tudi prihraniti stroške, ko ste v drugem omrežju. Če kljub temu želite spremeniti nastavitve, kliknite povezavo **Spremeni**.

Opomba:

Ta funkcija je na voljo le v sistemu Microsoft Windows 7.

Virusi in druga zlonamerna programska oprema

Zlonamerni programi so programi, ustvarjeni posebej za to, da poškodujejo računalnik, ga brez vaše privolitve uporabijo za nezakonite namene ali da ukradejo podatke, shranjene v njem.

Zlonamerna programska oprema lahko:

- prevzame nadzor nad spletnim brskalnikom,
- preusmeri poskuse iskanja,
- prikazuje neželene oglase,
- sledi, katera spletna mesta obiskujete,
- ukrade osebne podatke, na primer podatke o bančnih računih,
- uporabi računalnik za pošiljanje neželene pošte,
- uporabi računalnik za napad na druge računalnike.

Zlonamerni programi lahko prav tako upočasnijo računalnik in ogrozijo njegovo stabilnost. Znamenje okužbe z *zlonamerno programsko opremo* je, če se delovanje računalnika nenadoma zelo upočasni ali se sistem pogosto zruši.

Virusi

Virus je po navadi program, ki se lahko priloži datotekam in se vedno znova podvaja ter spreminja ali nadomesti vsebino drugih datotek, s čimer poškoduje računalnik.

Virus se običajno namesti v računalnik brez vaše vednosti. Ko je enkrat v računalniku, se poskuša replicirati. Virus:

- uporablja sistemska sredstva računalnika,
- lahko spremeni ali poškoduje datoteke v računalniku,
- pogosto poskuša računalnik uporabiti za to, da okuži še druge računalnike,
- lahko omogoči, da zlonamerni uporabniki računalnik uporabijo v nezakonite namene.

Vohunski programi

Vohunski programi zbirajo osebne podatke.

Vohunski programi zbirajo osebne podatke, vključno z informacijami o:

- obiskanih spletnih mestih,
- e-poštnih naslovih v vašem računalniku,
- geslih,
- številkah kreditnih kartic.

Vohunska programska oprema se skoraj vedno namesti samodejno brez vašega izrecnega dovoljenja. Lahko se namesti tudi skupaj z uporabnim programom ali pa vas prelisiči z zavajajočim pojavnim oknom, v katerem kliknete določeno možnost.

Korenski kompleti

Korenski kompleti so programi, zaradi katerih je drugo *zlonamerno programsko opremo* težko najti.

Korenski kompleti skrijejo datoteke in procese. To običajno naredijo zato, da skrijejo zlonamerno dejavnost v računalniku. Kadar korenski komplet skriva *zlonamerno programsko opremo*, je zelo težko zaznati, da je računalnik okužen.

Ta izdelek vsebuje poseben iskalnik korenskih kompletov, zato se *zlonamerni programi* težje skrijejo.

Tvegana programska oprema

Tvegana programska oprema ni izdelana posebej zato, da bi škodovala računalniku, vendar pa lahko kljub temu poškoduje računalnik, če je ne uporabljate pravilno.

Tvegani programi niso nujno tudi zlonamerni. Izvajajo nekatere funkcije, ki so sicer uporabne, vendar utegnejo biti nevarne.

Tvegani programi so na primer:

- programi za neposredna sporočila (na primer IRC),
- programi za prenos datotek prek interneta iz enega računalnika v drugega,
- programi za internetno telefonijo (VoIP ali *prenos govora po omrežju IP*).
- programi za oddaljeni dostop (na primer VNC),
- sleparski varnostni programi, ki posameznike prestrašijo ali preslepijo in jih tako prepričajo v nakup ponarejene varnostne opreme, ali
- programi, ki so bili razviti zato, da obidejo preverjanje CD-jev ali zaščito pred kopiranjem.

Če ste program namestili sami in ga pravilno nastavili, je manj verjetno, da bo poškodoval računalnik.

Če je bil tvegani program nameščen brez vaše privolitve, se je to najverjetneje zgodilo z namenom škodovati, zato ga morate odstraniti.

Poglavje

4

Varovanje računalnika pred zlonamerno programsko opremo

Teme:

- *Pregled računalnika*
- *Kako izključiti datoteke iz pregleda*
- *Uporaba karantene*
- *Kaj je DeepGuard?*

Z iskanjem virusov in vohunske programske opreme lahko varujete računalnik pred programi, ki bi utegnili krasti vaše osebne podatke, poškodovati računalnik ali ga uporabiti v nezakonite namene.

Privzeto se vsa zlonamerna programska oprema obravnava, takoj ko je najdena, tako da ne more povzročiti nobene škode.

Zaščita pred virusi in vohunsko programsko opremo privzeto omogoča pregled lokalnih trdih diskov, vseh izmenljivih medijev (kot so prenosni pogoni ali CD-ji) in samodejni prenos vsebine. Lahko jo nastavite tako, da omogoča tudi samodejno pregledovanje e-pošte.

S preverjanjem prisotnosti virusov in vohunske programske opreme se v računalniku preverijo tudi vse spremembe, ki bi lahko pomenile prisotnost *zlonamerne programske opreme*. Če so najdene kakršne koli nevarne sistemske spremembe, na primer nastavitev sistema ali poskusi spreminjanja pomembnih sistemskih procesov, DeepGuard prepreči zagon tega programa, saj gre verjetno za *zlonamerno programsko opremo*.

Pregled računalnika

Ko je vklopljena zaščita pred virusi in vohunskimi programi, ta samodejno išče škodljive datoteke v računalniku. Datoteke lahko pregledate tudi ročno in nastavite preglede po urniku.

Priporočamo, da je zaščita pred virusi in vohunskimi programi ves čas vklopljena. Datoteke preglejte ročno, če želite zagotoviti, da v računalniku ni škodljivih datotek ali če želite pregledati datoteke, ki ste jih izključili iz sprotnega pregleda.

Ko nastavite pregled po urniku, zaščita pred virusi in vohunskimi programi odstrani škodljive datoteke iz računalnika ob določenenih časovnih obdobjih.

Samodejno pregledovanje datotek

Sprotno pregledovanje ščiti računalnik tako, da sproti pregleduje vse datoteke, do katerih dostopate, in preprečuje dostop do datotek z *zlonamerno programsko opremo*.

Ko računalnik poskuša dostopati do datoteke, funkcija sprotnega pregledovanja najprej pregleda, ali je v datoteki prisotna zlonamerna programska oprema in šele nato omogoči računalniku dostop do datoteke. Če sprotno pregledovanje zazna kakršno koli zlonamerno programsko opremo, datoteko prenese v karanteno, preden ta lahko poškoduje računalnik.

Ali sprotno pregledovanje vpliva na učinkovitost delovanja računalnika?

Postopek pregledovanja po navadi ni moteč, ker ne traja dolgo in zahteva malo sistemskih sredstev. Koliko časa in sistemskih sredstev se porabi pri sprotnem pregledovanju, je na primer odvisno tudi od vsebine, mesta in vrste datoteke.

Datoteke, katerih pregled traja dlje časa:

- Datoteke na izmenljivih pogonih, na primer na pogonih CD, DVD ter na prenosnih pogonih USB.
- Stisnjene datoteke, na primer datoteke *.zip*.

  Opomba: Stisnjene datoteke niso privzeto pregledane.

Sprotno pregledovanje lahko upočasni delovanje računalnika:

- imate računalnik, ki ne ustreza sistemskim zahtevam, ali pa
- ste dostopali do več datotek hkrati. Na primer, ko odprete imeniz z več datotekami, ki jih je treba pregledati.

Vklop ali izklop funkcije za sprotno pregledovanje

Funkcijo sprotnega pregledovanja pustite vklopljeno, če želite *zlonamernim programom* preprečiti, da poškodujejo računalnik.

Če želite vklopiti ali izklopiti sprotno pregledovanje:

1. Na glavni strani kliknite **Stanje**.
2. Kliknite **Spremeni nastavitve na tej strani**.

   Opomba: Če želite izklopiti varnostne funkcije, potrebujete skrbniške pravice.

3. Vklopite ali izklopite funkcijo **Zaščita pred virusi in vohunskimi programi**.
4. Kliknite **Zapri**.

Samodejna obravnava škodljivih datotek

Sprotno pregledovanje omogoča samodejno obravnavanje škodljivih datotek brez vprašanj.

Če želite omogočiti samodejno obravnavanje škodljivih datotek pri sprotnem pregledovanju:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Varnost računalnika** > **Zaščita pred virusi in vohunskimi programi**.
3. Izberite **Samodejna obravnava škodljivih datotek**.

Če ne izberete možnosti samodejne obravnave škodljivih datotek, vas sprotno pregledovanje vpraša, kaj želite narediti, ko je najdena škodljiva datoteka.

Obravnava vohunskih programov

Zaščita pred virusi in vohunskimi programi blokira vohunski program takoj, ko se ta poskuša zagnati.

Preden se vohunski program lahko zažene, ga izdelek blokira in vam prepusti odločitev, kaj želite narediti.

Če je najden vohunski program, izvedite enega od teh dejanj:

Želeno dejanje	Kaj se zgodi z vohunskim programom
Obravnavaj samodejno	Izdelku prepustite odločitev, da sam izbere najboljši ukrep glede na najdeni vohunski program.
Premakni vohunski program v karanteno	Vohunski program premaknite v karanteno, kjer ne more škodovati računalniku.
Izbriši vohunski program	Iz računalnika odstranite vse datoteke, povezane z vohunskimi programi.
Blokiraj le vohunski program	Blokirajte dostop do vohunskega programa, a ga pustite v računalniku.
Izvzemi vohunski program iz pregleda	Vohunskemu programu dovolite izvajanje in ga v prihodnje izključite iz pregleda.

Obravnava tveganih programov

Zaščita pred virusi in vohunskimi programi blokira tvegani program takoj, ko se ta poskuša zagnati.

Preden se tvegani program lahko zažene, ga izdelek blokira in vam prepusti odločitev, kaj želite narediti.

Če je najden tvegani program, izvedite enega od teh dejanj:

Želeno dejanje	Kaj se zgodi s tveganim programom
Blokiraj le tvegani program	Blokirajte dostop do tveganega programa, a ga pustite v računalniku.
Premakni tvegani program v karanteno	Tvegani program premaknite v karanteno, kjer ne more škodovati računalniku.
Izbriši tvegani program	Iz računalnika odstranite vse datoteke, povezane s tveganimi programi.
Izvzemi tvegani program iz pregleda	Tveganemu programu dovolite izvajanje in ga v prihodnje izključite iz pregleda.

Samodejno odstranjevanje sledilnih piškotkov

Spletnim mestom lahko preprečite, da sledijo obiskanim spletnim mestom, tako da odstranite sledilne piškotke.

Sledilni piškotki so majhne datoteke, ki spletnim mestom omogočajo, da si zapomnijo obiskana spletna mesta. Če ne želite sledilnih piškotkov v vašem računalniku, sledite tem navodilom.

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Varnost računalnika** > **Zaščita pred virusi in vohunskimi programi**.
3. Izberite **Odstrani sledilne piškotke**.
4. Kliknite **V redu**.

Ročno pregledovanje datotek

Datoteke lahko pregledate tudi ročno, na primer, ko na računalnik priključite zunanjo napravo in želite zagotoviti, da ta ne vsebuje zlonamerne programske opreme.

Zagon ročnega pregleda

Pregledate lahko celoten računalnik ali pa iščete določeno vrsto *zlonamernega programa* ali določeno mesto.

Če sumite, da je računalnik okužen z določeno vrsto *zlonamerne programske opreme*, lahko iščete samo to vrsto. Če sumite, da je okuženo samo določeno mesto v računalniku, lahko pregledate samo to mesto. Delni pregled bo končan veliko hitreje kakor pregled celotnega računalnika.

Ročni pregled računalnika zaženete takole:

1. Na glavni strani kliknite puščico pod razdelkom **Pregled**.

   Prikažejo se možnosti pregleda.

2. Izberite vrsto pregleda.

   Izberite **Spremeni nastavitve pregledovanja**, če želite optimizirati ročno pregledovanje virusov in drugih škodljivih programov v računalniku.

3. Če se odločite za možnost **Izberite, kaj želite pregledati**, se odpre okno, v katerem izberete, katero mesto želite pregledati.
   Odpre se **Čarovnik za pregled**.

Hitro iskanje zlonamernih programov

Pregledate lahko celoten računalnik ali samo posamezno mesto, lahko pa poiščete tudi določeno vrsto zlonamernega programa.

V nadaljevanju so opisane različne vrste pregledov:

Vrsta pregleda	Kaj se pregleda	Kdaj uporabiti ta pregled
Iskanje virusov in vohunskih programov	Poišče viruse ter vohunske in tvegane programe v posameznih delih računalnika	Ta vrsta pregleda je veliko hitrejša od pregleda celotnega računalnika. Preišče le tisti del sistema, v katerem so nameščene programske datoteke. Priporočamo, da to iskanje uporabite, če želite hitro preveriti, ali je računalnik čist, saj ponuja učinkovito iskanje in odstranjevanje vseh aktivnih zlonamernih programov v računalniku.
Pregled celotnega računalnika	Poišče viruse ter vohunske in tvegane programe v celotnem računalniku (na notranjih in zunanjih trdih diskih)	Kadar se želite prepričati, da v računalniku zagotovo ni zlonamernih ali tveganih programov. Ta vrsta pregleda traja najdlje. Združuje hitro iskanje zlonamerne programske opreme in pregled trdih diskov. Pregleda tudi elemente, ki so morda skriti v korenskem kompletu.
Izberite, kaj želite pregledati	Poišče viruse ter vohunske in tvegane programe v določeni	Če sumite, da je neko mesto v računalniku okuženo z zlonamernim programom, na primer če so na tem mestu shranjene datoteke, prenesene iz morebitno

Vrsta pregleda	Kaj se pregleda	Kdaj uporabiti ta pregled
	datoteki, mapi ali na določenem pogonu	nevarnih virov, kot je na primer omrežje za izmenjavo datotek. Kako dolgo traja pregled, je odvisno od velikosti izbranega cilja. Če pregledate mapo, v kateri je nekaj manjših datotek, je pregled hitro gotov.
Iskanje korenskih kompletov	Pomembna mesta v sistemu, kjer bi lahko sumljiv element ogrozil varnost. Poišče skrite datoteke, mape, pogone ali procese	Če sumite, da je v računalniku nameščen korenski komplet. Na primer, če ste v računalniku pred kratkim odkrili zlonamerni program in se želite prepričati, da se ni namestil tudi korenski komplet.

Pregledovanje v raziskovalcu

V raziskovalcu operacijskega sistema Windows lahko na diskih, v datotekah in mapah iščete *viruse* ter *vohunske* in *tvegane programe*.

Disk, mapo ali datoteko pregledate takole:

1. Kazalec miške postavite na disk, mapo ali datoteko, ki jo želite pregledati, in kliknite z desno tipko.
2. V priročnem meniju izberite **Poišči viruse v mapah**. (Ukaz je odvisen od tega, ali pregledujete disk, mapo ali datoteko.)
   Odpre se okno **Čarovnik za pregled** in pregled se začne.

Če je najden *virus* ali *vohunski program*, vas **Čarovnik za pregled** vodi skozi postopek čiščenja.

Izbira datotek za pregled

Izberete lahko vrste datotek, v katerih želite iskati*viruse* in*vohunske programe* z ročnim ali razporejenim pregledovanjem.

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Druge nastavitve** > **Ročni pregled**.
3. V razdelku **Možnosti pregleda** lahko izbirate med temi nastavitvami:

Preglej le znane vrste datotek	Za pregled le tistih datotek, ki bodo najverjetneje okužene, na primer izvedljive datoteke. Z izbiro te možnosti pospešite pregled. Pregledane bodo datoteke s temi priponami: `.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` in `.hqx`.
Preglej stisnjene datoteke	Če želite pregledati arhivske datoteke in mape.
Uporabi napredno hevristiko	Če želite za pregled uporabiti vso razpoložljivo hevristiko, da boste lažje našli nove ali neznane zlonamerne programe **Opomba:** Če izberete to možnost, pregled traja dlje in lahko se zgodi, da bo najdenih več lažno pozitivnih datotek (neškodljive datoteke bodo prepoznane kot sumljive).

4. Kliknite V redu.

Opomba: Izvzete datoteke na seznamu izvzetih elementov niso pregledane, tudi če tukaj izberete njihov pregled.

Kaj storiti, ko so najdene škodljive datoteke?

Izberite način obravnavanja najdenih škodljivih datotek.

Če želite izbrati, katero dejanje naj se izvede, ko je med ročnim pregledom najdena škodljiva vsebina:

1. Na glavni strani kliknite Nastavitve.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite Druge nastavitve > Ročni pregled.
3. V razdelku Če je najden virus ali vohunska programska oprema izberite eno od teh možnosti:

Možnost	Opis
Vprašaj (privzeto)	Izberete lahko vrsto dejanja, ki naj se izvede za vsak element, ki je najden med ročnim pregledom.
Izbriši datoteke	Program skuša samodejno očistiti okužene datoteke, najdene pri ročnem pregledu. **Opomba:** Če izdelek ne more izbrisati okužene datoteke, jo premakne v karanteno (razen, če je najdena v omrežju ali na izmenljivih pogonih), da ne poškoduje računalnika.
Pošlji datoteke v karanteno	Izdelek premakne vse škodljive datoteke, ki so bile najdene pri ročnem pregledu, v karanteno, kjer ne morejo poškodovati računalnik.
Izbriši datoteke	Program izbriše vse škodljive datoteke, najdene pri ročnem pregledu.
Samo poročaj	Izdelek pusti vse škodljive datoteke, ki so bile najdene pri ročnem pregledu, kakršne so, v poročilo o pregledu pa zabeleži, kaj je bilo zaznano. **Opomba:** Če izberete to možnost, pa sprotno pregledovanje ni vklopljeno, lahko zlonamerna programska oprema vseeno poškoduje računalnik.

Opomba: Če so pri pregledovanju po urniku najdene škodljive datoteke, so samodejno izbrisane.

Razporedi pregled

Računalnik nastavite tako, da samodejno pregleduje in odstranjuje viruse in druge škodljive programe, ko ga ne uporabljate. Ali pa nastavite možnost rednega pregledovanja, da zagotovite, da je računalnik čist.

Če želite razporediti pregled:

1. Na glavni strani kliknite Nastavitve.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite Druge nastavitve > Načrtovani pregled.
3. Vklopite možnost Pregled po urniku.
4. Izberite, kdaj želite, da se začne pregled.

Možnost	Opis
Dnevno	Računalnik preglejte vsak dan.

Možnost	Opis
Tedensko	Računalnik preglejte na izbrane dni v tednu. Na seznamu izberite dneve.
Mesečno	Računalnik preglejte na izbrane dni v mesecu. Če želite izbrati dneve: 1. Izberite ustrezno možnost v razdelku Dan. 2. Na seznamu poleg izbranega dne izberite želeni dan v mesecu.

5. Izberite, kdaj želite, da se na izbrane dneve začne pregled.

Možnost	Opis
Začetni čas	Pregled zaženite ob določenem času.
Potem ko je računalnik nedejaven	Pregled zaženite, ko računalnika niste uporabljali določeno časovno obdobje.

Funkcija pregledovanja po urniku za pregledovanje računalnika uporablja nastavitve ročnega pregledovanja, vendar vsakokrat pregleda tudi arhive in samodejno izbriše škodljive datoteke.

Preglej e-pošto

Funkcija pregledovanja e-pošte vas zaščiti pred škodljivimi datotekami, ki jih prejmete v e-poštnih sporočilih.

Če želite pregledati e-pošto, ali so v njej virusi, mora biti zaščita pred virusi in škodljivimi programi vklopljena.

Če želite vklopiti pregledovanje e-pošte:

1. Na glavni strani kliknite Nastavitve.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite Varnost računalnika > Zaščita pred virusi in vohunskimi programi.
3. Izberite Odstrani škodljive e-poštne priloge.
4. Kliknite V redu.

Kdaj so pregledana e-poštna sporočila in priloge?

Z zaščito pred virusi in vohunskimi programi lahko odstranite škodljivo vsebino iz prejetih e-poštnih sporočil.

Zaščita pred virusi in vohunskimi programi odstrani škodljiva e-poštna sporočila, ki jih prejmete v e-poštnih programih, kot so Microsoft Outlook in Outlook Express, Microsoft Mail ali Mozilla Thunderbird. Orodje pregleda nešifrirana e-poštna sporočila in priloge vsakič, ko jih e-poštni program prek protokola POP3 prejme s poštnega strežnika.

Zaščita pred virusi in vohunskimi programi ne more pregledati e-poštna sporočila, poslana ali prejeta s spletnimi e-poštnimi programi, ki se izvajajo v spletnem brskalniku, kot so Hotmail, Yahoo! mail in Gmail. Še vedno ste zaščiteni pred *virusi*, tudi če ne odstranite škodljivih prilog ali če uporabljate spletno pošto. Ko odprete e-poštne priloge, funkcija sprotnega pregledovanja odstrani morebitne škodljive priloge, preden lahko povzročijo škodo.

Opomba: Sprotno pregledovanje omogoča zaščito le za vaš računalnik, ne pa tudi za vaše prijatelje. Sprotno pregledovanje ne pregleda pripetih datotek, če ne odprete priloge. Če uporabljate spletno pošto, to pomeni, da prijateljem lahko pošljete okuženo e-poštno sporočilo, če jim posredujete sporočilo, preden odprete prilogo.

Prikaz rezultatov pregleda

Zgodovina virusov in vohunskih programov prikazuje vse škodljive datoteke, ki jih je program našel.

Včasih izdelek ne more izvesti izbranega dejanja, če zazna škodljiv element. Na primer, če izberete brisanje datotek in datoteke ni mogoče izbrisati, izdelek premakne datoteko v karanteno. Te informacije si lahko ogledate v zgodovini virusov in vohunskih programov.

Če si želite ogledati zgodovino:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Varnost računalnika** > **Zaščita pred virusi in vohunskimi programi**.
3. Kliknite **Prikaži zgodovino brisanja**.

V zgodovini virusov in vohunskih programov so prikazane te informacije:

- datum in čas, ko je bila škodljiva datoteka najdena,
- ime zlonamerne programske opreme in njeno mesto v računalniku in
- izvedeno dejanje.

Kako izključiti datoteke iz pregleda

Včasih boste morda želeli iz pregleda izključiti nekatere datoteke ali programe. Izključeni elementi niso pregledani, razen če jih ne odstranite iz seznama izključenih elementov.

Opomba: Seznami izjem so ločeni od sprotnega in ročnega pregledovanja. Če na primer izključite datoteko iz sprotnega pregledovanja, je ta pregledana med ročnim pregledovanjem, razen če datoteke ne izključite tudi iz ročnega pregledovanja.

Izvzemanje vrst datotek

Ko izvzamete datoteke glede po njihovi vrsti, datoteke z določenimi prilogami ne bodo pregledane, ali se v njih nahaja škodljiva vsebina.

Če želite dodati ali odstraniti vrsto datoteke, ki jo želite izvzeti:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite, ali želite izvzeti vrsto datoteke iz sprotnega ali ročnega pregledovanja:
   - Izberite **Varnost računalnika** > **Zaščita pred virusi in vohunskimi programi**, če želite izvzeti vrsto datoteke iz sprotnega pregledovanja.
   - Izberite **Druge nastavitve** > **Ročni pregled**, če želite izvzeti vrsto datoteke iz ročnega pregledovanja.
3. Kliknite **Izvzemi datoteke iz pregleda**.
4. Če želite izvzeti vrsto datotek:
   a) Kliknite zavihek **Vrste datotek**.
   b) Izberite **Izvzemi priloge s temi priponami**.
   c) Vnesite pripono datoteke, ki določa vrsto datotek, ki jih želite izvzeti, v polju poleg gumba **Dodaj**.

      Če želite opredeliti datoteke brez pripone, vnesite ».«. Uporabite lahko nadomestni znak »?«, ki nadomešča poljuben znak, oziroma »*«, ki nadomešča poljubno število znakov.

      Če želite na primer izvzeti izvedljive datoteke, v polje vnesite `exe`.
   d) Kliknite **Dodaj**.
5. Prejšnji korak ponovite za vse pripone, ki jih želite izvzeti iz iskanja virusov.

6. Kliknite **V redu**, da zaprete pogovorno okno **Izvzemi iz pregleda**.
7. Kliknite **V redu**, da uporabite nove nastavitve.

Izbrane vrste datotek so izvzete iz prihodnjih pregledovanj.

Izvzemanje datotek glede na mesto

Ko izvzamete datoteke glede na mesto, datoteke na določenih pogonih ali v mapah ne bodo pregledane, ali se v njih nahaja škodljiva vsebina.

Če želite dodati ali odstraniti mesta datotek, ki jih želite izvzeti:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite, ali želite izvzeti mesto iz sprotnega ali ročnega pregledovanja:
   - Izberite **Računalnik** > **Zaščita pred virusi in vohunskimi programi**, če želite izvzeti mesto iz sprotnega pregledovanja.
   - Izberite **Računalnik** > **Ročno pregledovanje**, če želite izvzeti mesto iz ročnega pregledovanja.
3. Kliknite **Izvzemi datoteke iz pregleda**.
4. Če želite izvzeti datoteko, pogon ali mapo:
   a) Izberite zavihek **Predmeti**.
   b) Izberite **Izvzemi predmete (datoteke, mape...)**.
   c) Kliknite **Dodaj**.
   d) Izberite datoteko, pogon ali mapo, ki jo želite izvzeti iz iskanja virusov.

      Opomba: Pogoni so lahko izmenljivi, na primer pogoni CD, DVD ali omrežni pogoni. Omrežnih pogonov in praznih izmenljivih pogonov ni mogoče izvzeti iz pregledovanja.

   e) Kliknite **V redu**.
5. Prejšnji korak ponovite za vse datoteke, pogone in mape, ki jih želite izvzeti iz iskanja virusov.
6. Kliknite **V redu**, da zaprete pogovorno okno **Izvzemi iz pregleda**.
7. Kliknite **V redu**, da uveljavite nove nastavitve.

Izbrane datoteke, pogoni ali mape so izvzete iz prihodnjih pregledov.

Ogled izvzetih programov

Oglejte si programe, ki ste jih izvzeli iz pregledovanja, in jih odstranite s seznama izvzetih elementov, če jih želite v prihodnje vključiti v pregledovanje.

Če je pri sprotnem ali ročnem pregledovanju zaznan program, ki se vede kot vohunski ali tvegani program, vendar veste, da je varen, ga lahko izvzamete iz pregleda, da vas izdelek nanj ne bo več opozarjal.

Opomba: Če se program vede kot virus ali druga zlonamerna programska oprema, je ni mogoče izvzeti.

Programov ne morete neposredno izvzeti. Novi programi so prikazani na seznamu izjem le, če jih izključite med pregledovanjem.

Če si želite ogledati programe, ki so izvzeti iz pregledovanja:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite, ali si želite ogledati programe, ki so bili izvzeti iz sprotnega ali ročnega pregledovanja.

- Izberite **Računalnik** > **Zaščita pred virusi in vohunskimi programi**, če si želite ogledati programe, ki so bili izvzeti iz sprotnega pregledovanja.
- Izberite **Računalnik** > **Ročno pregledovanje**, če si želite ogledati programe, ki so bili izvzeti iz ročnega pregledovanja.

3. Kliknite **Izvzemi datoteke iz pregleda**.
4. Izberite zavihek **Programi**.

   Opomba: Izvzeti je mogoče samo vohunsko in tvegano programsko opremo, ne pa tudi virusov.

5. Če želite znova pregledati izvzeti program:
   a) Izberite program, ki ga želite vključiti v pregled.
   b) Kliknite **Odstrani**.
6. Kliknite **V redu**, da zaprete pogovorno okno **Izvzemi iz pregleda**.
7. Kliknite **V redu**, da zaprete program.

Uporaba karantene

Karantena je varno mesto za datoteke, ki bi lahko poškodovale računalnik.

Datoteke v karanteni se ne morejo širiti ali škodovati računalniku.

V karanteno lahko premaknete *zlonamerne*, *vohunske* in *tvegane* programe, da ne bodo škodovali računalniku. Če jih kdaj pozneje potrebujete, jih lahko obnovite.

Če elementa v karanteni ne potrebujete, ga lahko izbrišete. S tem ga trajno odstranite iz računalnika.

- V splošnem lahko *zlonamerno programsko opremo* v karanteni izbrišete.
- V večini primerov lahko izbrišete *vohunske programe* v karanteni. *Vohunski program* v karanteni je lahko del povsem običajnega programa, ki morda ne bo več deloval, če ga izbrišete. Če želite ta program ohraniti, *vohunski program* obnovite iz karantene.
- *Tvegani programi* v karanteni so lahko povsem neškodljivi. Če ste jih namestili in nastavili sami, jih lahko obnovite iz karantene. Če je bil *tvegani program* nameščen brez vaše privolitve, se je to najverjetneje zgodilo z namenom škodovati, zato ga morate izbrisati.

Ogled elementov v karanteni

Če želite, si lahko ogledate dodatne informacije o elementih v karanteni.

Podrobne informacije o elementih v karanteni prikažete takole:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Varnost računalnika** > **Zaščita pred virusi in vohunskimi programi**.
3. Kliknite **Prikaži karanteno**.
   Na strani **Karantena** je prikazano skupno število elementov, shranjenih v karanteni.
4. Če si želite ogledati podrobne informacije o elementih v karanteni, kliknite **Podrobnosti**.

   Vsebino lahko razvrstite po imenu zlonamerne programske opreme ali po poti datoteke.

   Prikaže se seznam prvih 100 elementov z vrsto elementov v karanteni, njihovimi imeni in potjo do mesta, kjer so datoteke nameščene.
5. Če si želite ogledati več informacij o elementu v karanteni, kliknite ikono ob elementu v stolpcu **Stanje**.

Obnavljanje elementov v karanteni

Iz karantene lahko obnovite elemente, ki jih potrebujete.

Programe ali datoteke v karanteni lahko obnovite, če jih potrebujete. Elementov, za katere niste prepričani, da so varni, ne obnavljajte. Obnovljeni elementi so premaknjeni na prvotno mesto v računalniku.

Obnavljanje elementov v karanteni

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Varnost računalnika** > **Zaščita pred virusi in vohunskimi programi**.
3. Kliknite **Prikaži karanteno**.
4. Izberite elemente v karanteni, ki jih želite obnoviti.
5. Kliknite **Obnovi**.

Kaj je DeepGuard?

DeepGuard analizira vsebino datotek in način delovanja programov ter nadzoruje programe, ki niso zaupanja vredni.

DeepGuard blokira nove in neodkrite *viruse*, *črve* ter druge škodljive programe, ki poskusijo spremeniti nastavitve v vašem računalniku, sumljivim programom pa prepreči dostop do interneta.

Ko DeepGuard zazna nov program, ki poskuša poskuša spremeniti sistemske nastavitve, ki bi lahko bile škodljive, pusti, da se ta program izvaja v varnem območju. Če se program izvaja v varnem območju, ne more poškodovati računalnika. DeepGuard analizira spremembe, ki jih je program poskusil izvesti, in na osnovi tega odloči, kako verjetno je, da gre za *zlonamerno programsko opremo*. Če je verjetno, da je program *zlonameren*, ga DeepGuard blokira.

Morebitne škodljive spremembe sistema, ki jih zazna DeepGuard, so:

- spremembe sistemskih nastavitev (registra sistema Windows),
- poskusi zapiranja pomembnih sistemskih programov, na primer varnostnih programov, kot je ta izdelek,
- poskusi urejanja pomembnih sistemskih datotek.

Vklop ali izklop programa DeepGuard

DeepGuard pustite vklopljen, če želite sumljivim programom preprečiti morebitne škodljive sistemske spremembe v računalniku.

Preden vklopite tehnologijo DeepGuard, se prepričajte, da je nameščen servisni paket SP2, če uporabljate Windows XP.

Če želite vklopiti ali izklopiti DeepGuard:

1. Na glavni strani kliknite **Stanje**.
2. Kliknite **Spremeni nastavitve na tej strani**.

   Opomba: Če želite izklopiti varnostne funkcije, potrebujete skrbniške pravice.

3. Vklopite ali izklopite **DeepGuard**.
4. Kliknite **Zapri**.

Dovoli programe, ki jih tehnologija DeepGuard preprečuje

Nadzorujete lahko, katere programe tehnologija DeepGuard dovoli in blokira.

Včasih tehnologija DeepGuard morda preprečuje zagon varnega programa, čeprav program želite uporabljati in veste, da je varen. To se zgodi, ker program poskuša narediti sistemske spremembe, ki so morda lahko škodljive. Morda ste program nenamerno preprečili, ko je bilo prikazano pojavno okno tehnologije DeepGuard.

Če želite dovoliti program, ki ga je DeepGuard blokiral:

1. Na glavni strani kliknite **Orodja**.
2. Kliknite **Programi**.
   Prikaže se seznam **Nadzorovani programi**.
3. Poiščite program, ki ga želite dovoliti.

   Opomba: Če želite razvrstiti seznam, lahko kliknete naslove stolpcev. Na primer, kliknite stolpec **Dovoljenje**, da seznam razvrstite na skupini dovoljenih in prepovedanih programov.

4. V stolpcu **Dovoljenje** izberite možnost **Dovoli**.
5. Kliknite **Zapri**.

DeepGuard programu znova dovoli izvajanje sistemskih sprememb.

Uporabi DeepGuard v združljivostnem načinu

Za optimalno zaščito DeepGuard začasno spremeni zagon programov. Nekateri programi omogočajo preverjanje poškodb ali sprememb v njih in morda niso združljivi s to funkcijo. Ob zagonu na primer spletnih iger z orodji za zaščito pred goljufijami, se na primer prepriča, da te niso bile kakor koli spremenjene. V teh primerih lahko vklopite združljivostni način.

Če želite vklopiti združljivostni način:

1. Na glavni strani kliknite **Nastavitve**.

   Opomba: Za spreminjanje nastavitev potrebujete skrbniške pravice.

2. Izberite **Varnost računalnika** > **DeepGuard**.
3. Izberite **Uporabi združljivostni način**.
4. Kliknite **V redu**.

Kako obravnavati opozorila o sumljivem delovanju

DeepGuard nadzoruje programe, ki niso zaupanja vredni. Če nadzorovani program poskuša dostopiti do interneta, poskuša spremeniti nastavitve v računalniku ali deluje sumljivo, ga DeepGuard blokira.

Ko v nastavitvah programa DeepGuard izberete možnost **Opozori me o sumljivem delovanju**, vas DeepGuard obvesti, ko zazna morebitno škodljivi program ali ko zaženete program neznanega ugleda.

Če želite izbrati, kako ravnati s programom, ki ga je blokiral DeepGuard:

1. Kliknite **Podrobnosti**, če si želite ogledati informacije o programu.
   V razdelku s podrobnostmi so prikazani ti podatki:
   - mesto programa,
   - ugled programa v omrežju z zaščito v realnem času in
   - pogostost programa.
2. Izberite, ali želite zaupati programu, ki ga je DeepGuard blokiral:

- Izberite **Programu zaupam. Omogoči dejanje.**, če ne želite blokirati programa.

  Program je najverjetneje varen, če:

  - je DeepGuard blokiral program kot posledico nečesa, kar ste naredili,
  - prepoznate program ali
  - ste program dobili od zaupanja vrednega vira.

- Izberite **Programu ne zaupam. Blokiraj ga.**, če želite ohraniti program blokiran.

  Program je najverjetneje nevaren, če:

  - je program nobičajen,
  - ima program neznan ugled ali
  - ne prepoznate programa.

3. Če želite omogočiti posredovanje sumljivega programa v analizo:

a) Kliknite **Pošlji poročilo o programu družbi F-Secure**.
Izdelek prikazuje pogoje za pošiljanje.

b) Kliknite **Sprejmi**, če se strinjate s pogoji in želite poslati vzorec.

Priporočamo, da vzorec pošljete, če:

- DeepGuard blokira program, za katerega veste, da je varen ali
- sumite, da je program *zlonamerna programska oprema*.