# F-secure Internet Security

## Koji su sistemski zahtevi za F-Secure Internet Security?

Koraci pre instalacije proizvoda:

- Proverite da li imate konekciju sa internetom u cilju validacije elektronskog ključa za aktivaciju, kao i preuzimanja ažuriranja/update-a.
- Omogućite Javascript u podešavanjima pretraživaća da biste aktivirali block pages u pretraživaču

**Preporučujemo instalaciju samo jednog antivirus software-a. U suprotom može doći do problema sa performansama računara.**

Podržane Windows verzije:

- Windows 10* sa poslednjom verzijom ažuriranja
- Windows 8.1*
- Windows 7 (SP1)

Nisu podržani ARM tableti.

Sistemski zahtevi:

- Processor: Intel Pentium 4 ili noviji
- RAM memorija: 1GB ili više
- Prostor na disku: 600 MB slobodnog prostora na disku

## Kako da instaliram F-Secure Internet Security?

Pre instalacije F-secure Internet Security budite sigurni da:

- Je Windows ažuriran
- Da ste deinstalirali nekompatibilni softver (program) drugog proizvodjača
- Da vaš Windows nalog ima administratorska prava
- Imate internet konekciju

1. Idite na preuzimanje Internet Security stranicu
2. Pronadjite Internet Security proizvod, kliknite na „Download for Windows“
3. U zavisnosti od pretraživača:

- Instalacioni fajl će automatski biti preuzet
- Ili ćete dobiti pitanje da sačuvate fajl, u tom slučaju kliknite na „Save file“

4. Izborom Ctrl+J na tastaturi otvoriće se folder u kome se nalazi preuzeti fajl

5. Dupli klik na instalacioni fajl:

- F-SecureNetworkInstaller-IS.exe (F-Secure Internet Security)

6. Kada se instalacioni prozor otvori, izaberite „Accept and continue“

7. Kad se zatraži, unesite ključ za aktivaciju koji vam je dostavljen (xxxx-xxxx-xxxx-xxxx-xxxx), izaberite „Next“ kako bi dovršili instalaciju.

- Proverite da li koristite tačan elektronski ključ. Za svaki Windows računar koristi se poseban/jedinstven elektronski ključ.

Dopustite da proizvod dovrši instalaciju. Instalacija traje nekoliko minuta (u zavisnosti od brzine internet veze), kada je F-Secure Internet Security instaliran, računar je zaštićen.

## Napredna podešavanja

Da bi ste otvorili ikonicu F-Secure u Windows taskbar-u, pratite uputstvo:

- Desni klik na ikonicu proizvoda u Windows taskbar-u. Ukoliko je ikonica proizvoda sakrivena, prvo kliknite na „Show hidden icons“ strelicu u taskbar-u.
- Meni sadrži sledeće

**Link to online portal - Otvara portal na kojem možete upravljati svojim nalogom**
**Gaming mode - Oslobadja sistemske resurse dok igrate igrice**
**Check for updates - Poverite i preuzmite najnovija ažuriranja**
**View messages - Prikaz bitnih notifikacija koje mogu zahtevati vašu pažnju**
**View recent events - Prikazuje radnje koje je proizvod preduzeo radi zaštite vašeg računara.**
**Open settings - Podešavanje proizvoda**
**About - Prikazuje verziju proizvoda**

## Kako da isključim sve sigurnosne funkcije?

Ukoliko želiš da oslobodiš sistemske resurse, možeš isključiti sigurnosne funkcije.
Sve funkcije će automatski biti pokrenute prilikom prvog sledećeg restarta računara. Takodje, manuelno ih možeš opet pokrenuti na glavnom prozoru proizvoda.

**Morate imati administratorska prava na računaru kako bi isključili sigurnosne funkcije. Računar neće biti u potpunosti zaštićen kada su isključene sigurnosne funkcije.**

- Na glavnom prozoru, izaberi „Tools“
- Izaberi „Turn off all security features“

## Legenda statusa zaštite

| Status | Značenje | Opis |
|---|---|---|
|  | Ok | Računar je zaštićen. Sve funkcije su uključene i rade ispravno. |
|  | Upozorenje | Računar nije u potpunosti zaštićen. Proizvod zahteva toju pažnju, npr. nije ažuriran duže vreme ili su isključene sigurnosne funkcije. |
|  | Error | Računar nije zaštićen. Proizvod zahteva hitnu akciju, npr. važne funkcije su isključene ili je pretplata istekla. |

Primeri statusnih poruka koje možete videti:

- Google Chrome browser extension is not in use
- Mozilla Firefox browser extension is not in use
- Internet Explorer browser extension is not in use
- Your subscription has expired

## Pregled skorašnjih dogadjaja

Možete proveriti na koji način proizvod štiti računar na „Event history“ stranici.

„Event history“ sadrži mogobrojne prikaze dogadjaja u vezi instaliranih proizvoda sa detaljima sigurnostnih mera koje je proizvod izvršio. Na primer, prikazuje zlonamerne dogadjaje koje je detektovao, obrisao ili prebacio u karantin.

- Na glavnom prozoru, izaberi „Tools“
- Izaberi „Recent events“

Pristupate „Event history“ stranici

„Event history“ prikazuje vreme i opis za svaki dogadjaj. U zavisnosti od vrste dogadjaja, možeš proveriti više detalja. Na primer, za zlonamerne fajlove možeš videti sledeće inforamcije:

- Datum i vreme kada je znolamerni fajl pronadjen
- Naziv malware-a i lokaciju na računaru, i
- Akciju koju je proizvod izvršio

## Promena podešavanja notifikacija

- Desni klik na F-secure ikonicu

Pojaviće se pop-up meni

- Izaberite „Open settings“

Prozor „Settings“ će se otvoriti

- Izaberite „Notifications“
- Izaberite „Show useful tips and updates“

Kada su notifikacije u podešavanjima uključene proizvod šalje obaveštanja o novostima, trikovima, specijalnim ponudama. Važne notifikacije su uvek aktivne i prikazane čak i kada notifikacije nisu uključene.

## Gaming mode

Da biste uključili gaming mode:

- Desni klik na F-secure ikonicu

Pojaviće se pop-up meni

- Izaberite „Gaming mode“
-

Upotreba sistemskih resursa je sada optimizovana, tako da igrica može neometano da radi.
Ne zaboravite da isključite „gaming mode“ nakon što zaustavite igricu. „Gaming mode“ će se automatski isključiti nakon restarta računara.

## Zaštitite svoj računar od zlonamernog sadržaja

Zlonamerne aplikacije i fajlovi mogu pokušati da oštete podatke na računaru, ili neovlašćeno pristupe sistemu računara kako bi ukrali tvoje privatne podatke

**Više informacija:** **Unwanted applications, Worms, Trojans, Backdoors, Exploits, Exploit kits**

## Real-time skeniranje

Real-time skeniranje štiti računar skeniranjem svih datoteka kada im se pristupa kao i blokiranjem pristupa onim datotekama koje sadrže zlonamerni softver.
Kada računar pokušava da pristupi datoteci, skeniranje u realnom vremenu skenira datoteku zbog zlonamjernog softvera, pre nego što omogući vašem računaru da pristupi datoteci.
Ako skeniranje u realnom vremenu pronadje neki štetni sadržaj, datoteku će prebaciti u karantin pre nego što se prouzrokuje šteta.
Da li skeniranje u realnom vremenu utiče na performanse mog računara?
U najvećem broju slučajeva neće primetiti proces skeniranja jer oduzima malo vremena i resursa sistema. Količina vremena i sistemskih resursa za skeniranje u realnom vremenu zavisi od na primer, sadržaja, lokacije i vrste datoteke.

Podaci koji se nalaze na CD-ovima, DVD-ovima i prenosivi USB uredjaji zahtevaju duže vreme za skeniranje.

**Kompresovani fajlovi, kao što su .zip fajlovi se ne skeniraju real-time skenerom**

Skeniranje u realnom vremenu može da uspori računar ako:

- imate računar koji ne ispunjava sistemske zahteve, ili
- pristupate velikom broju datoteka istovremeno. Na primer, kada otvorite direktorijum koji sadrži mnogo datoteka koje je potrebno skenirati.

- Antivirus stanica, izaberi„Settings“
- Izaberi „Viruses and Threats“
- Uključite „Virus Protection“

## Kako da pokrenem skeniranje virusa?

Kako bi ste bili sigurni da nema zlonamernih fajlova ili neželjenih aplikacija na računaru

- Na glavnom prozoru, izaberi „Tools“
- „Virus scan options“
- Ukoliko želiš da optimizuješ manulano način na koji se vrši skeniranje, izaberi „Change scanning settings“

**Morate imati administratorska prava na računaru kako bi isključio sigurnosne funkcije.**

- Izaberi **„Scan only known file types"** za fajlove za koje postoji veća verovatnoća da budu zlonamernni, npr. executable fajlova. Skeniranje samo poznatih vrsta fajlova ubrzava skeniranje.

Fajlovi sa sledećim ekstenizijama su primeri poznatih fajl tipova: com, doc, exe, htm, ini, jar, pdf, scr, wma, xml, zip.

- **„Scan inside compressed files"** za skeniranje fajlova koje se nalaze u komprimovanim arhivskim fajlovima, na primer zip datoteke. Skeniranje unutar komprimovanih datoteka čini skeniranje sporijim. Ostavite opciju neoznačenu za skeniranje arhivske datoteke, ali ne i datoteke koje se nalaze u njoj.
- Izaberi **„OK"** kao bi ste se vratili na „Tools" stranicu

- Izaberi **„Virus scan"** ili **„Full computer scan"**

„Virus scan" skenira samo delove sistema koji sadrže instalirane aplikacije, može pronaći i ukloniti neželjene aplikacije kako i zlonamerne fajlove na računaru za kraće vreme.
„Full computer scan" skenira interne i eksterne hard diskove na viruse, spyware, potencijalno neželjene aplikacije, takodje proverava da li potencijalno postoje pretnje sakrivene u sootkit-u. Full computer scan računara može trajati duže.

Ukoliko proizvod u toku skeniranja pronadje zlonamerni program, sve detekcije će biti izlistane
Odabirom detektovane pretnje možete izabrati na koji način želite da obradjujete detekovani štetni sadržaj

| Opcije | Opis |
|---|---|
| Clean up | Uklanja fajlove automatski. Falovi koji se ne mogu ukloniti, smeštaju se u kartantin. |
| Quarantine | Premešta zlonamerne fajlove na bezbedno mesto sa kog se ne mogu da se proširiti ili naštetiti računaru. |
| Delete | Trajno uklanja fajlove sa računara. |
| Skip | Trenutno nema akcije, fajl ostaje na računaru za sada. |
| Exclude | Dozvoli aplikaciiji da radi i izostavi je u narednim skeniranjima. |

**Neke opcije nisu dostupne za sve štetne sadržaje.**

- Izaberi **„Handle all"** kako bi započeli proces uklanjanja

Nakon skeniranja prikazani su krajnji rezultati kao i broj zlonamernog sadržaja koji je uklonjen

**Napomena: Skeniranje virusa može zahtevati restart računara kako bi završio proces čišćenja. Ukoliko proizvod zahteva restart, izaberite Restart kako bi uklonili štetni sardržaj**

Krajnji rezultat možete proveriti odabirom **„Open last scanning report"**

## Skeniranje Windows operativnog sistema

Možete skenirati particije, foldere, fajlove i neželjene aplikacije u Windows Explorer-u.

Da bi skenirali particiju, folder ili fajl:
- Desni klik na particiju, folder ili fajl koji želite da skenirate
- Iz menija koji je prikazan desnim klikom, izaberite „Scan for viruses"

Skeniranje virusa počinje i skenira se particija, foldera ili fajla koji ste izabrali.

Zakazano skeniranje - Podesite računar da automatski skenira i uklanja viruse i druge štetne aplikacije kada ga ne koristite, ili podesite da se skeniranje periodično izvodi.

Slanje uzorka – Možete pomoći u boljoj zaštiti i dostaviti sumnjivi sadržaj na analizu proizvodjaču

## Šta je DeepGuard?

DeepGuard prati aplikacije kako bi otkrio potencijalno štetne promene u sistemu.

DeepGuard osigurava da koristite samo sigurne aplikacije. Sigurnost aplikacije se potvrdjuje iz pouzdanog servisa u oblaku. Ako se sigurnost aplikacije ne može proveriti, DeepGuard započinje praćenje ponašanja aplikacije.
DeepGuard blokira nove i neotkrivene trojans, worms, exploits i druge štetne aplikacije koje pokušavaju da izvrše promene na računaru i sprečavaju sumnjive aplikacije da pristupe internetu.

Potencijalno štetne promene sistema koje DeepGuard detektira uključuju:
System setting (Windows registry) podešavanja
Pokušaj da se isključe važni sistemski programi, npr. security programi kao što je i ovaj
Pokušaj izmene važnih sistemskih fajlova

Kako bi bili sigurni da je DeepGuard aktivan:
- Na stranici Antivirus, izaberi **„Settings"**

**Morate imati administratorska prava na računaru kako bi mogli da izvršite izmene.**

- **"Viruses and Threats"**
- **"Turn on DeepGuard"**

Kada je DeepGuard uključen, automatski blokira zlonamerne aplikacije koje potencijalno pokušavaju da vrše izmene na sistemu.

## Korišćenje kontrole aplikacija i fajlova

Možete da pregledate i upravljate aplikacijama i fajlovima koje proizvod blokira u prikazu **App and file control.**
Prikaz kontrole aplikacija i fajlova sadrži opise.

Karantin
Vratite stavke iz karantina
Izuzeti fajlove i foldere iz sekeniranja *Kada iz skeniranja izuzmete fajlove i foldere, oni se ne skeniraju na zlonamerni sadržaj
Provera izuzetih fajlova i foldera
Kontrolišite koje aplikacije DeepGuard blokira
Možete odabrati koji folderi zahtevaju dodatni sloj zaštite od zlonamernog softvera, kao što je **ransomvare**.
Sprečite aplikacije da preuzimaju zlonamerne fajlove

## Blokiranje zlonamernih sajtova

**Browsing protection** blokira pristup štetnim sajtovima kada je uključen.

Kako uključiti Browsing protection
Blokiranje sumnjivih i zabranjenih sajtova
Korišćenje ikona za ocenu reputacije sajta
Šta raditi kada je sajt blokiran
Dopuštanje i blokiranje odredjenog sajta

## Sigurno online bankarstvo

**Banking protection** dodaje još jedan nivo bezbednosti kako bi sprečio napadače da ometaju poverljive transakcije, kao i od zlonamernih aktivnosti kada pristupate intenet banci ili dok vršite transakcije online.

Banking protection automatski aktivira sigurnu vezu sa sajtom banke i blokira sve ostale konekcije koje nisu konekcija sa sajtom banke. Kada otvorite sajt banke, dozvoljene su samo konekcije sa online bankarstvom ili konekcijama koje se smatraju bezbednim za internet bankarstvo.

Banking protection trenutno podržava sledeće pretraživače:
Internet Explorer 11 ili noviji
Microsoft Edge
Firefox 13 ili noviji
Google Chrome

- Aktiviranje Banking protection
- Korišćenje online banking zaštite
- Provera koje ekstenzije pretraživača su u upotrebi

## Kako da uključim roditeljski nadzor na računaru deteta uz pomoć F-secure Internet Security?

Pratite aktivnosti deteta online i postavite ograničenja uredjaja kao i sadržaj pomoću funkcije **Parental control.**

**Ako vaše dete ima pristup porodičnom računaru, napravite zaseban Windows nalog za dete, prijavite se na taj nalog, a zatim sledite ove iste korake.**

- Ulogujte se na računar
- Otvorite Internet Secuirty
- Izaberite "**Parental control**"> "**Turn on"**, a zatim "**Yes"** da biste aktivirali roditeljski nadzor

Sledeća podešavanja su podrazumevano uključena:
**Content blocking** - Blokiranje sadržaja
**Device use limits** - Ograničenja upotrebe uredjaja

Pristup podešavanjima

- Idite na dno glavnog prikaza proizvoda koji sadrži tekst: "**You can change these from settings i izaberite settings".**

- Ako je potrebno, unesite svoja administratorska prava na računaru i izaberite "**Yes"**. Ovim otvarate podešavanja za roditeljski nadzor.

Podešavanja su sledeća:

**Content blocker** - omogućava blokiranje sajtova na osnovu njihovog sadržaja ili omogućava pristup samo odredjenim sajtovima.
**Search result filter** - postavlja Google, Yahoo, YouTube, i Bing na "strogi" nivo koji sakriva sadržaj za odrasle kao i njihov prikaz u rezultatima pretrage.
**Device use limits** - omogućava ograničenje koliko dugo i kada vaše dete može da koristi računar ili pretražuje internet.
Definišite podešavanja koja želite za računar vašeg deteta /account and/or enable/disable settings, izaberite **OK.**

## Kako mogu da ograničim vreme koje moje dete provodi na računaru koristeći funkciju Parental Control?

**Ako vaše dete ima pristup porodičnom računaru, napravite zaseban Windows nalog za dete, prijavite se na taj nalog, a zatim sledite ove iste korake.**

- Ulogujte se na računar
- Otvorite Internet Secuirty

Pristup podešavanjima

- Idite na dno glavnog prikaza proizvoda koji sadrži tekst: "You can change these from settings i izaberite settings".
- Ako je potrebno, unesite svoja administratorska prava na računaru i izaberite "Yes".

Sa leve strane izaberite Device use limits

- Navedite kada tokom dana vaše dete može biti za računarom; na primer, 2 sata ujutru i 2 sata uveče pre spavanja.
- Navedite ukupan broj sati dnevno

**Kada se dostigne vremensko ograničenje za taj dan, računar se zaključava.**

- Kliknite na OK, kako bi potvrdili podešavanja.

## Kako mogu da blokiram sajtove pomoću funkcije Parental control?

Tražite način da zaštitite svoju porodicu od sajtova koje sadrže neprikladan sadržaj? Budite sigurni i aktivirajte Content blocker.

**Pre postavljanja vremenskih ograničenja, prvo uključite Parental control funkciju**

- Ulogujte se na računar
- Otvorite Internet Secuirty

Pristup podešavanjima

- Idite na dno glavnog prikaza proizvoda koji sadrži tekst: "You can change these from settings i izaberite settings".

- Ako je potrebno, unesite svoja administratorska prava na računaru i izaberite **"Yes"**.

- Sa leve strane izaberite **Content blocker**

Blokiranje web sadržaja prema vrsti sadržaja

- Izaberite **Block web content**

Potvrdite izbor u polju pored tipova sadržaja koje želite da blokirate za korisnika

Dozvolite pristup samo odredjenim sajtovima

- Izaberite **Allow only selected web sites**
- Kliknite na Add unesite web stranicu koju želite da omogućite korisniku. Pritisnite **OK**. Ponovite ovaj korak da za svaki sadržaj koji želite da dodate.

Kliknite na **OK**, kako bi potvrdili podešavanja.

Vrste sadržaja

## Šta je firewall?

Firewall sprečava „upad" štetnog sadržaja sa interneta na računar i omogućava samo sigurne internet konekcije sa računara.

Promena podešavanja Windows Firewall
Korišćenje ličnih Firewall-a

## Automatska ažuriranja

Automatska ažuriranja čuvaju računar od najnovijih pretnji.

Provera poslednjeg automatskog ažuriranja
Uputstvo o tome kako da promenite način na koji se računar povezuje na internet i kako želite da preuzimate ažurirnja tokom korišćenja mobilnih mreža

## Kako da obnovim F-secure Internet Security?

Obratite se prodavcu od koga ste kupili proizvod

## Kako da aktviram elektronski ključ nakon obnavljanja F-secure Internet Security?

Aktiviranje koda

- Otvorite F-Secure Internet Security
- Na vrhu prozora  sa desne strane odaberite **Already have a new subscription code?**.
- Ispod opisa **Renew subscription Enter subscription code** unesite kod za pretplatu
- Izaberite **Continue**.

Vaša pretplata se obnavljena.

## Obnovio/la sam F-Secure Internet Security, ali ne mogu da pronađem ključ za pretplatu F-secure Internet Security. Gde ga mogu pronaći?

Dobili ste elektronski ključ putem email-a. Pronadjite email i pronadjite ključ za aktivaciju.

Ključ je u sledećem formatu: AAAA-BBBB-1111-CCCC-2222.

Pomoću ključa možete nastaviti sa aktiviranjem obnove.

## Kako da prebacim instalaciju (ili licencu) na drugi računar?

Ako ste prilikom instaliranja F-Secure Internet Security iskoristili raspoloživu licencu, prizvod zadržava ključ kao korišćenu licencu, pre aktiviranja licence na drugom računaru morate deinstalirati proizvod sa računara na kom je proizvod trenutno instaliran.

**Pre deinstalacije pronadjite mail u kom vam je dostavljen ključ za aktivaciju, kao bi mogli da ga upotrebite na drugom računaru.**

**Privacy**
**Tehnička podrška**