Kaspersky Internet Security

UPORABNIŠKA NAVODILA

RAZLIČICA APLIKACIJE: 15.0 MAINTENANCE RELEASE 1

KAZALO

GLAVNE LASTNOSTI APLIKACIJE

Kaspersky Internet Security zagotavlja celovito zaščito računalnika pred znanimi in novimi grožnjami, omrežnimi napadi in napadi ribarjenja ter neželeno elektronsko pošto. Kot del rešitve Kaspersky Internet Security so na voljo številne funkcije in komponente, ki skupaj nudijo celovito zaščito.

Zaščita računalnika

Komponente zaščite so namenjene zaščiti računalnika pred že znanimi in novimi grožnjami, omrežnimi napadi, goljufijami in neželeno pošto. Za vsako vrsto grožnje poskrbi posamezna komponenta zaščite (glej opis komponent v tem poglavju). Komponente je mogoče vklopiti ali izklopiti neodvisno eno od druge, mogoče pa je tudi prilagoditi njihove nastavitve.

Poleg zaščite v realnem času, ki jo zagotavljajo komponente zaščite, priporočamo, da redno pregledujete svoj računalnik za odkrivanje morebitnih virusov ali druge škodljive programske opreme. To je potrebno, da preprečite morebitno širitev škodljivih programov, ki jih niso zaznale komponente zaščite, na primer zato, ker je bila nastavljena nizka raven zaščite, ali iz drugih razlogov.

Rešitev Kaspersky Internet Security posodobite tako, da posodobite podatkovne zbirke in programske module, ki jih uporablja aplikacija.

Nekatere specifične naloge, ki jih je treba občasno izvajati (npr. odstranitev sledi uporabnikovih aktivnosti v operacijskem sistemu), se izvajajo z uporabo *naprednih orodij in čarovnikov*.

Naslednje komponente zaščite skrbijo za zaščito vašega računalnika v realnem času:

Sledi opis logike, ki stoji za interakcijo komponent zaščite, ko je rešitev Kaspersky Internet Security nastavljena na način, ki ga priporočajo strokovnjaki podjetja Kaspersky Lab (ko torej uporablja privzete nastavitve aplikacije).

Protivirusna zaščita za datoteke (File Anti-Virus)

Protivirusna zaščita za datoteke preprečuje okužbe datotečnega sistema računalnika. Komponenta se zažene ob zagonu operacijskega sistema, stalno deluje v pomnilniku in pregleduje vse datoteke, ki jih odprete, shranite ali zaženete s svojega računalnika ali kateregakoli povezanega pogona. Kaspersky Internet Security prestreže vsak poskus dostopa do datoteke in pregleda datoteko, da preveri, če vsebuje katerega od znanih virusov ali drugih škodljivih programov. Nadaljnji dostop do datoteke je mogoč le, če datoteka ni okužena ali jo je aplikacija uspešno očistila. Če datoteke iz kakršnegakoli razloga ni mogoče očistiti, je izbrisana. V takšnem primeru je kopija datoteke shranjena v karanteno.

Protivirusna zaščita za elektronsko pošto (Mail Anti-Virus)

Protivirusna zaščita za elektronsko pošto pregleduje prejeta in poslana elektronska sporočila na vašem računalniku. Prejemnik ima dostop do sporočila le, če ne vsebuje nevarnih elementov.

Protivirusna zaščita na spletu (Web Anti-Virus)

Protivirusna zaščita na spletu prestreže in zaustavi izvajanje skript na spletnih straneh, če predstavljajo grožnjo. Hkrati spremlja ves spletni promet in preprečuje dostop do nevarnih spletnih mest.

Protivirusna zaščita za takojšnje sporočanje (IM Anti-Virus)

Protivirusna zaščita za takojšnje sporočanje zagotavlja varno uporabo sistemov takojšnjega sporočanja. Komponenta ščiti informacije, ki prihajajo do vašega računalnika prek protokolov takojšnjega sporočanja. Zagotavlja varno delovanje številnih aplikacij za takojšnje sporočanje.

Nadzor aplikacij (Application Control)

Nadzor aplikacij beleži aktivnosti aplikacij v operacijskem sistemu in te aktivnosti upravlja glede na skupino, v katero je komponenta uvrstila posamezno aplikacijo. Za vsako skupino aplikacij veljajo posebna pravila. Ta pravila urejajo dostop aplikacij do različnih virov operacijskega sistema

Požarna pregrada (Firewall)

Požarna pregrada skrbi za vašo zaščito, ko uporabljate lokalna omrežja in internet. Komponenta filtrira vse omrežne aktivnosti z uporabo dveh vrst pravil: pravila za aplikacije in pravila za pakete.

Nadzornik omrežja (Network Monitor)

Nadzornik omrežja je zasnovan za spremljanje aktivnosti v omrežju v realnem času.

Nadzor sistema (System Watcher)

Komponento za nadzor sistema je mogoče uporabiti za razveljavljanje aktivnosti škodljive programske opreme v operacijskem sistemu.

Preprečevanje napadov iz omrežja (Network Attack Blocker)

Komponenta za preprečevanje napadov iz omrežja se naloži ob zagonu operacijskega sistema in spremlja dohodni omrežni promet, če bi zaznal kakšno aktivnost, ki je značilna za omrežne napade. Ko zazna poskus napada na vaš računalnik, rešitev Kaspersky Internet Security prepreči vse omrežne aktivnosti iz napadalnega računalnika, usmerjene proti vašemu računalniku.

Zaščita pred neželeno pošto (Anti-Spam)

Zaščita pred neželeno pošto je vgrajena v odjemalca e-pošte, ki je nameščen na vašem računalniku, in pregleduje vsa dohodna elektronska sporočila, da odkrije morebitno neželeno pošto. Vsa tovrstna sporočila so označena s posebno oznako. Nastavitve komponente za zaščito pred neželeno pošto lahko poljubno urejate glede na to, kaj želite, da se z neželenimi sporočili zgodi (npr. samodejno se izbrišejo ali pa so prestavljena v posebno mapo).

Zaščita pred napadi ribarjenja (Anti-Phishing)

Zaščita pred napadi ribarjenja omogoča preverjanje naslovov URL, da ugotovi, ali je določen naslov vključen v seznam ponarejenih naslovov. Ta komponenta je vgrajena v komponente za protivirusno zaščito na spletu, zaščito pred neželeno pošto in protivirusno zaščito za takojšnje sporočanje.

Zaščita pred oglaševanjem (Anti-Banner)

Zaščita pred oglaševanjem blokira oglase na spletnih straneh in v vmesnikih aplikacij.

Safe Money

Komponenta Safe Money zagotavlja zaščito zaupnih podatkov pri uporabi bančnih storitev in plačilnih sistemov ter preprečuje krajo pri spletnih plačilih.

Varen vnos podatkov prek tipkovnice (Secure Keyboard Input)

Komponenta za varen vnos podatkov prek tipkovnice zagotavlja zaščito pred programi za beleženje tipkovnice za osebne podatke, ki jih vnašate na spletnih straneh. Virtualna tipkovnica preprečuje, da bi bili podatki, vneseni prek fizične tipkovnice, prestreženi, in ščiti osebne podatke pred poskusi, da bi bili podatki prestreženi z uporabo posnetkov zaslona.

Način zaupanja vrednih aplikacij (Trusted Applications)

Način zaupanja vrednih aplikacij računalnik ščiti pred aplikacijami, ki so morda nevarne. Ko je ta način vklopljen, rešitev Kaspersky Internet Security omogoča le uporabo aplikacij, ki so določene kot zaupanja vredne (na primer na podlagi informacij o aplikaciji iz omrežja KSN ali zaupanja vrednega digitalnega podpisa).

Starševski nadzor (Parental Control)

Starševski nadzor je namenjen zaščiti otrok in najstnikov pred grožnjami, povezanimi z uporabo računalnika in interneta.

Omogoča vam, da nastavite prilagodljive omejitve dostopa do spletnih virov in aplikacij za različne uporabnike glede na njihovo starost. Poleg tega vam starševski nadzor omogoča ogled statističnih poročil o aktivnostih nadzorovanih uporabnikov.

Sodelovanje v programu Zaščitite prijatelja

S sodelovanjem v programu Zaščitite prijatelja boste prejeli bonus točke, ko boste delili povezave do rešitve Kaspersky Internet Security s svojimi prijatelji. Svoje bonus točke lahko zamenjate za dodatno kodo za aktivacijo za rešitev Kaspersky Internet Security.

Posodabljanje podatkovnih zbirk in modulov programske opreme

Rešitev Kaspersky Internet Security v privzetem načinu samodejno preverja, ali so na strežnikih podjetja Kaspersky Lab na voljo posodobitve. Če strežnik vsebuje nabor nedavnih posodobitev, jih rešitev Kaspersky Internet Security prenese in namesti v ozadju. Posodobitev za Kaspersky Internet Security lahko kadarkoli zaženete ročno, in sicer iz glavnega okna aplikacije ali iz priročnega menija ikone aplikacije v območju za obvestila opravilne vrstice.

Za prenos posodobitev s strežnikov za posodobitve podjetja Kaspersky Lab je potrebna povezava z internetom.

V sistemu Microsoft Windows 8 se posodobitve ne bodo prenesle, če je vzpostavljena širokopasovna internetna povezava in je v aplikaciji nastavljena omejitev prometa prek tovrstne povezave. Za prenos posodobitev morate ročno izklopiti omejitev, kar storite v oknu z nastavitvami aplikacije, v pododseku z nastavitvami omrežja **Network**.

- *Za zagon posodobitve iz priročnega menija ikone aplikacije v območju za obvestila opravilne vrstice:*

  V priročnem meniju ikone aplikacije izberite vnos **Update**.

- *Za zagon posodobitve iz glavnega okna aplikacije:*

  1. Odprite glavno okno aplikacije in kliknite gumb **Update**.

     V oknu se prikaže odsek **Update**.

  2. V odseku **Update** kliknite gumb **Run update**.

PREGLEDOVANJE RAČUNALNIKA

To poglavje podaja informacije o tem, kako preveriti, ali računalnik vsebuje viruse ali druge grožnje.

V TEM POGLAVJU

POPOLN PREGLED

Med popolnim pregledom Kaspersky Internet Security privzeto pregleda naslednje elemente:

- Sistemski pomnilnik
- Elemente, ki se naložijo ob zagonu operacijskega sistema
- Nosilce podatkov
- Trde diske in zunanje diske

Priporočamo, da takoj po namestitvi rešitve Kaspersky Internet Security na svoj računalnik zaženete popoln pregled.

Za začetek popolnega pregleda:

1. Odprite glavno okno aplikacije.
2. Kliknite gumb **Scan**.

   Odpre se okno za pregled računalnika (**Scan**).
3. V oknu **Scan** izberite odsek **Full Scan** (popoln pregled).
4. V odseku **Full Scan** kliknite gumb **Run scan** za zagon pregleda.

Kaspersky Internet Security začne s popolnim pregledom vašega računalnika.

PRILAGOJEN PREGLED

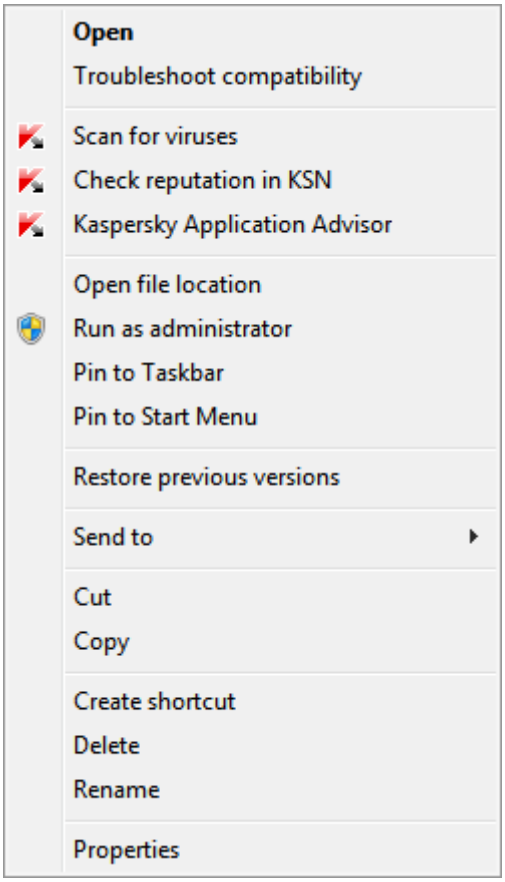
Prilagojen pregled omogoča pregled posamezne datoteke, mape ali pogona, da preverite, ali morebiti vsebuje viruse ali druge grožnje.

Prilagojen pregled lahko sprožite na naslednje načine:

- Iz priročnega menija elementa
- Iz glavnega okna aplikacije

Za zagon pregleda iz priročnega menija elementa:

1. Odprite Raziskovalca in poiščite mapo, v kateri se nahaja element, ki ga želite pregledati.
2. Z desnim klikom odprite priročni meni elementa (glej spodnjo sliko) in izberite možnost **Scan for viruses**.



Slika 2. Priročni meni elementa

Za zagon pregleda iz glavnega okna aplikacije:

1. Odprite glavno okno aplikacije.
2. Kliknite gumb **Scan**.

   Odpre se okno za pregled računalnika (**Scan**).
3. V oknu **Scan** izberite odsek **Custom Scan** (prilagojen pregled).
4. Na enega od naslednjih načinov izberite element, ki ga želite pregledati:
   - Povlecite elemente v okno **Custom Scan**.
   - Kliknite gumb **Add** in v oknu s seznamom datotek ali map, ki se odpre, izberite želeni element.
5. Kliknite gumb **Run scan** za začetek pregleda.

HITRI PREGLED

Med hitrim pregledom Kaspersky Internet Security privzeto pregleda naslednje elemente:

- Elemente, ki se naložijo ob zagonu operacijskega sistema
- Sistemski pomnilnik
- Zagonski sektor na trdem disku

Za zagon hitrega pregleda:

1. Odprite glavno okno aplikacije.
2. Kliknite gumb **Scan**.

   Odpre se okno za pregled računalnika (**Scan**).
3. V oknu **Scan** izberite odsek **Quick Scan** (hitri pregled).
4. V odseku **Quick Scan** kliknite gumb **Run scan** za zagon pregleda.

Kaspersky Internet Security začne s hitrim pregledom vašega računalnika.

PREGLED VERJETNO OKUŽENIH DATOTEK

Če sumite, da je določena datoteka okužena, jo preglejte z rešitvijo Kaspersky Internet Security (glej poglavje Prilagojen pregled na strani 7).

Če aplikacija zaključi pregled in sporoči, da je datoteka varna, kljub temu pa sumite, da ni, jo lahko pošljete raziskovalni ekipi Virus Lab. Strokovnjaki za viruse iz skupine Virus Lab pregledajo datoteko. Če se izkaže, da je okužena z virusom ali predstavlja drugačno grožnjo, dodajo opis novega virusa v podatkovne zbirke. Aplikacija prenese podatkovne zbirke med vsako posodobitvijo podatkovnih zbirk in modulov programske opreme (glej poglavje Posodabljanje podatkovnih zbirk in modulov programske opreme na strani 6).

Če želite poslati datoteko skupini Virus Lab:

1. Obiščite spletno stran za zahteve Virus Lab (http://support.kaspersky.com/virlab/helpdesk.html).
2. Sledite navodilom na tej strani, ki vas bodo usmerjala pri pošiljanju vaše zahteve.

ODKRIVANJE VARNOSTNIH POMANJKLJIVOSTI

Varnostne pomanjkljivosti so nezaščiteni deli programske kode, ki jih lahko napadalci izkoristijo za lastne namene, na primer za kopiranje podatkov, uporabljenih v nezaščitenih aplikacijah. Iskanje varnostnih pomanjkljivosti na računalniku vam pomaga odkriti morebitne šibke točke v varnosti vašega računalnika. Priporočeno je, da tovrstne odkrite pomanjkljivosti odpravite.

Za zagon pregleda za odkrivanje varnostnih pomanjkljivosti:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo Show Additional Tools za prikaz dodatnih orodij. Odpre se okno z orodji (Tools).
3. V levem delu okna Tools kliknite na povezavo Vulnerability Scan, da se odpre okno Vulnerability Scan za odkrivanje varnostnih pomanjkljivosti.
4. V oknu Vulnerability Scan kliknite gumb Run scan za zagon pregleda.

Kaspersky Internet Security začne pregledovati vaš računalnik, da odkrije morebitne varnostne pomanjkljivosti.

ZAŠČITA ELEKTRONSKE POŠTE

To poglavje podaja informacije o tem, kako elektronsko pošto zaščititi pred neželenimi sporočili, virusi in drugimi grožnjami.

V TEM POGLAVJU

NASTAVITEV PROTIVIRUSNE ZAŠČITE ZA E-POŠTO

Kaspersky Internet Security s protivirusno zaščito za elektronsko pošto (Mail Anti-Virus) omogoča pregledovanje e-poštnih sporočil in iskanje nevarnih elementov. Protivirusna zaščita za elektronsko pošto se zažene ob zagonu operacijskega sistema in je ves čas naložena v pomnilniku ter pregleduje vsa sporočila, poslana ali prejeta preko protokolov POP3, SMTP, IMAP, MAPI in NNTP, kar vključuje pošto, poslano preko varnih povezav (SSL) preko protokolov POP3, SMTP in IMAP.

Privzeto protivirusna zaščita za e-pošto pregleduje prejeta in poslana sporočila. Če želite, lahko vklopite pregledovanje le prejete pošte.

Koraki za nastavitev protivirusne zaščite za elektronsko pošto:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu okna kliknite na povezavo z nastavitvami (**Settings**).
3. V levem delu okna v odseku **Protection** izberite komponento za protivirusno zaščito za elektronsko pošto (**Mail Anti-Virus**).

   V oknu se odprejo nastavitve.
4. Prepričajte se, da je vklopljeno stikalo v zgornjem delu okna, s kateri vklopite/izklopite protivirusno zaščito za elektronsko pošto.
5. Izberite raven varnosti:
   - **Recommended**. Če izberete to raven, bo protivirusna zaščita pregledovala prejeta in poslana sporočila ter pripete arhivske datoteke.
   - **Low**. Če izberete to raven, bo protivirusna zaščita pregledovala prejeta sporočila brez pregledovanja pripetih arhivskih datotek.
   - **High**. Če izberete to raven, bo protivirusna zaščita pregledovala prejeta in poslana sporočila ter pripete arhivske datoteke. Pri najvišji ravni zaščite (High) bo vklopljena tudi poglobljena hevristična analiza.
6. Na spustnem seznamu **Action on threat detection** izberite aktivnost, ki naj jo zažene protivirusna zaščita, ko odkrije okužen element (na primer, očisti datoteko).

Če v e-poštnem sporočilu ni odkritih groženj ali pa so bili vsi okuženi elementi uspešno očiščeni, bo sporočilo na voljo za nadaljnjo uporabo. Če komponenta ne uspe očistiti okuženega elementa, bo protivirusna zaščita za e-pošto ta element preimenovala ali izbrisala iz sporočila in v zadevo sporočila dodala obvestilo, da je sporočilo obdelala rešitev Kaspersky Internet Security. Pred izbrisom elementa rešitev Kaspersky Internet Security naredi varnostno kopijo in jo prestavi v karanteno (Quarantine) (glej poglavje Obnova elementa, ki ga je aplikacija izbrisala ali očistila na strani 10).

BLOKIRANJE NEŽELENE POŠTE

Če prejmete velike količine neželene pošte, vklopite komponento za zaščito pred neželeno pošto (Anti-Spam) in nastavite priporočeno raven varnosti.

Koraki za vklop možnosti za zaščito pred neželeno pošto in izbiro priporočene ravni varnosti:

7. Odprite glavno okno aplikacije.
8. V spodnjem delu okna kliknite na povezavo z nastavitvami (**Settings**). Odprite odsek **Settings**.
9. V levem delu okna izberite odsek **Protection**.
10. V levem delu okna v odseku **Protection** izberite komponento za zaščito pred neželeno pošto (**Anti-Spam**).

    V oknu se odprejo nastavitve zaščite pred neželeno pošto.
11. V desnem delu okna s stikalom vklopite zaščito pred neželeno pošto.
12. V odseku **Security level** izberite priporočeno raven zaščite - **Recommended**.

ZAŠČITA OSEBNIH PODATKOV NA INTERNETU

V tem poglavju so podane informacije o tem, kako zagotoviti varno brskanje po spletu in kako zaščititi svoje podatke pred krajo.

V TEM POGLAVJU

O ZAŠČITI OSEBNIH PODATKOV NA INTERNETU

Kaspersky Internet Security vam pomaga zaščititi osebne podatke pred krajo:

- Gesla, uporabniška imena in druge podatke za prijavo
- Številke računov in bančnih kartic

Kaspersky Internet Security vključuje komponente in orodja, s katerimi lahko svoje osebne podatke zaščitite pred poizkusi kraje z metodami, kot sta ribarjenje in prestrezanje podatkov, vpisanih preko tipkovnice.

Zaščito pred napadi ribarjenja zagotavlja možnost Anti-Phishing, ki je vgrajena v komponente za protivirusno zaščito na spletu (Web Anti-Virus), zaščito pred neželeno pošto (Anti-Spam) in protivirusno zaščito za takojšnje sporočanje (IM Anti-Virus). Z vklopom teh komponent si lahko zagotovite celovito zaščito pred napadi ribarjenja.

Zaščito pred prestrezanjem podatkov, vnesenih preko tipkovnice, zagotavljata virtualna tipkovnica (Virtual Keyboard) in varen vnos podatkov prek tipkovnice (Secure Keyboard Input).

Čarovnik Privacy Cleaner Wizard očisti računalnik vseh podatkov o aktivnostih uporabnika.

Možnost Safe Money ščiti podatke, ko uporabljate storitve internetnega bančništva in kupujete v spletnih trgovinah.

Zaščito pred prenosom osebnih podatkov prek interneta zagotavlja eno od orodij za starševski nadzor (Parental Control) - glej poglavje Uporaba starševskega nadzora na strani 26.

O VIRTUALNI TIPKOVNICI

Ko uporabljate internet, morate pogosto vpisovati svoje osebne podatke ali svoje uporabniško ime in geslo. To se na primer dogaja pri registraciji računa na spletnih straneh, pri spletnem nakupovanju in pri elektronskem bančništvu.

Obstaja tveganje, da bodo te osebne informacije prestrežene s strojno ali programsko opremo, ki beleži pritiske na tipke. Virtualna tipkovnica je orodje, ki preprečuje prestrezanje podatkov, vpisanih preko tipkovnice.

Številni programi, ki sodijo med vohunsko programsko opremo, lahko delajo posnetke zaslona, ki se nato samodejno prenesejo vsiljivcu v nadaljnjo analizo z namenom kraje osebnih podatkov. Virtualna tipkovnica ščiti vnesene osebne podatke pred poskusi kraje z uporabo posnetkov zaslona.

Virtualna tipkovnica ima naslednje lastnosti:

- Gumbe virtualne tipkovnice lahko klikate z miško.
- Za razliko od tipk na fizični tipkovnici, na virtualni tipkovnici ni mogoče hkrati pritisniti na več tipk. Zato kombinacije tipk (kot so **ALT+F4**) od vas zahtevajo, da najprej kliknete na prvo tipko (na primer **ALT**), nato na drugo (na primer **F4**) in nato znova na prvo. Drugi klik na tipko ima enak učinek, kot če na fizični tipkovnici spustimo tipko.
- Jezik virtualne tipkovnice je mogoče spreminjati z uporabo iste bližnjice, kot je določena v nastavitvah operacijskega sistema za fizično tipkovnico. To storimo z desnim klikom na drugo tipko (če je na primer v operacijskem sistemu za zamenjavo jezika tipkovnice nastavljena bližnjica **LEVI ALT+SHIFT**, z levim klikom izberite tipko **LEVI ALT**, nato pa z desnim klikom tipko **SHIFT**).

Da zagotovite zaščito podatkov, vnesenih prek virtualne tipkovnice, po namestitvi rešitve Kaspersky Internet Security ponovno zaženite računalnik.

Uporaba virtualne tipkovnice ima naslednje omejitve:

- Virtualna tipkovnica preprečuje prestrezanje osebnih podatkov le, ko jo uporabljate z brskalnikom Microsoft Internet Explorer, Mozilla Firefox ali Google Chrome. Če jo uporabljate z drugim brskalnikom, virtualna tipkovnica ne bo zaščitila vnesenih osebnih podatkov pred prestrezanjem.
- Možnost virtualne tipkovnice ni na voljo v brskalnikih Microsoft Internet Explorer 10 in 11 z vmesnikom Modern ali v brskalnikih Microsoft Internet Explorer 10 in 11 z vklopljenim **Izboljšanim zaščitenim načinom**. V tem primeru priporočamo, da odprete virtualno tipkovnico iz vmesnika rešitve Kaspersky Internet Security.
- Virtualna tipkovnica ne more zaščititi vaših osebnih podatkov, če so spletno stran, na kateri ste vpisali svoje podatke, napadli hekerji, ki tovrstne podatke pridobijo neposredno iz podatkovnih zbirk.
- Virtualna tipkovnica ne preprečuje posnetkov zaslona, narejenih z uporabo tipke **PRINT SCREEN** in drugih kombinacij tipk, ki so določene v nastavitvah operacijskega sistema.
- Ko deluje virtualna tipkovnica, možnost Samodokončanje brskalnika Microsoft Internet Explorer preneha delovati, saj bi uporaba samodejnega vnosa kriminalcem lahko omogočila, da prestrežejo podatke.
- V nekaterih brskalnikih (kot je Google Chrome) zaščita vnosa podatkov morda ne bo delovala za nekatere vrste podatkov (kot so na primer elektronski naslovi ali števila).

Zgornji seznam opisuje glavne omejitve funkcionalnosti za zaščito vnosa podatkov. Celoten seznam omejitev je na voljo v članku na spletni strani tehnične podpore Kaspersky Lab http://support.kaspersky.com/11047.

ZAGON VIRTUALNE TIPKOVNICE

Virtualno tipkovnico lahko odprete na naslednje načine:

- Iz priročnega menija ikone aplikacije v območju za obvestila opravilne vrstice
- Iz glavnega okna aplikacije
- Iz okna brskalnika Microsoft Internet Explorer, Mozilla Firefox ali Google Chrome, tako da kliknete na ikono za hitri dostop do virtualne tipkovnice

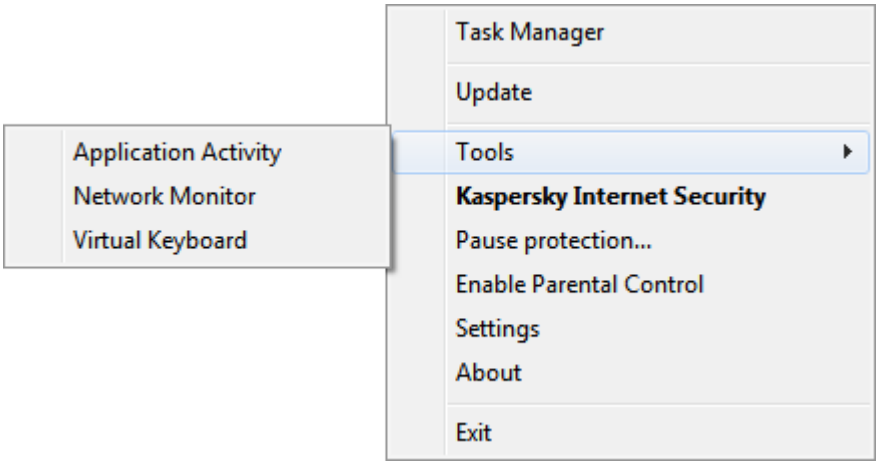
Nastavite lahko prikaz ikone za hitri zagon virtualne tipkovnice v poljih za vnos na spletnih straneh.

Ko uporabljate virtualno tipkovnico, Kaspersky Internet Security izklopi možnost samodokončanja v poljih za vnos na spletnih straneh.

- S pritiskom na kombinacijo tipk na tipkovnici.

Za zagon virtualne tipkovnice iz priročnega menija ikone aplikacije v območju za obvestila opravilne vrstice:

V priročnem meniju ikone aplikacije (glej spodnjo sliko) izberite **Tools** → **Virtual Keyboard**.



Slika 3. Priročni meni aplikacije Kaspersky Internet Security

Za zagon virtualne tipkovnice iz glavnega okna aplikacije:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo **Show Additional Tools** za prikaz dodatnih orodij. Odpre se okno z orodji **(Tools)**.
3. V levem delu okna **Tools** kliknite na povezavo **Virtual Keyboard**, da odprete virtualno tipkovnico.

Za zagon virtualne tipkovnice iz okna brskalnika:

Kliknite gumb 

Virtual Keyboard v orodni vrstici brskalnika Microsoft Internet Explorer, Mozilla Firefox ali Google Chrome.

Za zagon virtualne tipkovnice z uporabo fizične tipkovnice:

Pritisnite bližnjico **CTRL**+**ALT**+**SHIFT**+**P**.

Koraki za nastavitev prikaza ikone za hitri zagon virtualne tipkovnice v poljih za vnos na spletnih straneh:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu okna kliknite na povezavo z nastavitvami **(Settings)**.
3. V oknu **Settings**, ki se odpre, v odseku **Additional** izberite **Secure Data Input**.

   Okno prikaže nastavitve za varen vnos podatkov.
4. Če je potrebno, v odseku **Virtual Keyboard** izberite potrditveno polje **Open Virtual Keyboard by typing CTRL+ALT+SHIFT+P** za zagon virtualne tipkovnice z uporabo zgornje bližnjice.

5. Če želite, da bo v poljih za vnos prikazana ikona za hitri zagon virtualne tipkovnice, izberite potrditveno polje **Show quick launch icon in data entry fields**.

6. Če želite, da bo ikona za hitri zagon virtualne tipkovnice prikazana le ob dostopu do določenih spletnih strani:

   a. V odseku **Virtual Keyboard** kliknite na povezavo **Edit categories**, da se odpre okno z nastavitvami varnega vnosa podatkov (**Secure Data Input settings**).

   b. Izberite potrditvena polja kategorij spletnih strani, pri katerih želite, da se v poljih za vnos pojavi ikona za hitri zagon virtualne tipkovnice.

      Ikona za hitri zagon virtualne tipkovnice se bo prikazala vsakič, ko boste naložili spletno stran, ki pripada eni od izbranih kategorij.

   c. Če želite vklopiti ali izklopiti prikaz ikone za hitri zagon virtualne tipkovnice na določeni spletni strani:

      a. Kliknite na povezavo **Configure exclusions**, da se odpre okno **Exclusions for Virtual Keyboard**, kjer določite izjeme za virtualno tipkovnico.

      b. V spodnjem delu okna kliknite gumb **Add**.

         Odprlo se bo okno za dodajanje izjem za virtualno tipkovnico.

      c. V polje **Website address mask** vnesite naslov spletne strani.

      d. Če želite, da bo ikona za hitri zagon virtualne tipkovnice prikazana (ali da ne bo prikazana) le na določeni spletni strani, v odseku **Scope** izberite **Apply to the specified page**.

      e. V odseku **Virtual Keyboard icon** določite, ali naj bo ikona za hitri zagon virtualne tipkovnice prikazana na določeni spletni strani.

      f. Kliknite gumb **Add**.

         Določena spletna stran se bo pojavila na seznamu v oknu **Exclusions for Virtual Keyboard**, kjer so naštete izjeme za virtualno tipkovnico.

Ko boste naložili izbrano spletno stran, bo prikazana ikona za hitri zagon virtualne tipkovnice, v skladu z izbranimi nastavitvami.

ZAŠČITA PODATKOV, VNESENIH PREK RAČUNALNIŠKE TIPKOVNICE

Zaščita podatkov, vpisanih preko računalniške tipkovnice, vam omogoča, da preprečite prestrezanje podatkov, ki ste jih vpisali preko tipkovnice.

Varen vnos podatkov prek tipkovnice (Secure Keyboard Input) ima naslednje omejitve:

- Zaščita podatkov, ki jih vnesete preko računalniške tipkovnice, je na voljo le za brskalnike Microsoft Internet Explorer, Mozilla Firefox in Google Chrome. Ko uporabljate druge spletne brskalnike, podatki, vneseni na ta način, ne bodo zaščiteni pred prestrezanjem.

- Varen vnos podatkov prek tipkovnice ni na voljo v brskalniku Microsoft Internet Explorer iz trgovine Windows.

- Zaščita podatkov, ki jih vnesete preko računalniške tipkovnice, ne more zaščititi vaših osebnih podatkov, če je bila stran, ki zahteva vnos teh podatkov, napadena, saj v tem primeru informacije napadalci dobijo neposredno s spletne strani.

- V nekaterih brskalnikih (kot je Google Chrome) zaščita vnosa podatkov morda ne bo delovala za nekatere vrste podatkov (kot so na primer elektronski naslovi ali števila).

Zgornji seznam opisuje glavne omejitve funkcionalnosti za zaščito vnosa podatkov. Celoten seznam omejitev je na voljo v članku na spletni strani tehnične podpore Kaspersky Lab http://support.kaspersky.com/11047.

Zaščito vnosa podatkov preko računalniške tipkovnice lahko nastavljate na številnih spletnih straneh. Ko enkrat nastavite zaščito vnosa podatkov prek računalniške tipkovnice, vam ni treba pri vnosu podatkov storiti nič drugega.

Za nastavitev zaščite vnosa podatkov prek računalniške tipkovnice:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu okna kliknite na povezavo z nastavitvami **(Settings)**. Pojdite v odsek **Settings**.
3. V odseku **Additional** izberite pododsek **Secure Data Input**.

   Okno prikaže nastavitve za varen vnos podatkov.
4. V spodnjem delu okna, v odseku **Secure Keyboard Input**, izberite potrditveno polje **Enable Secure Keyboard Input**.
5. Določite vrsto zaščite za vnos podatkov preko fizične tipkovnice:
   a. Odprite okno **Secure Data Input settings**, tako da kliknete na povezavo **Edit categories** v spodnjem delu odseka **Secure Keyboard Input**.
   b. Izberite kategorije spletnih strani, na katerih želite zaščititi podatke, ki jih vnašate preko tipkovnice.
   c. Če želite na določeni strani vključiti zaščito podatkov, vnesenih preko tipkovnice:
      a. Odprite okno **Exclusions for Secure Keyboard Input**, tako da kliknete na povezavo **Configure exclusions**.
      b. V oknu kliknite gumb **Add**.

         Odpre se okno, kjer lahko dodate izjeme za varen vnos podatkov prek tipkovnice.
      c. V oknu, ki se odpre, v polje **Website address mask** vnesite naslov spletne strani.
      d. Izberite eno od možnosti za varen vnos podatkov na tej spletni strani (**Apply to the specified page**, če želite, da nastavitev velja samo za določeno stran, ali **Apply to the entire website**, če želite, da nastavitev velja za celotno spletno mesto).
      e. Izberite, kako naj možnost varnega vnosa podatkov ravna na tej spletni strani (**Protect** (Zaščiti) ali **Do not protect** (Ne zaščiti)).
      f. Kliknite gumb **Add**.

Izbrana spletna stran se bo pojavila na seznamu izjem v oknu **Exclusions for Secure Keyboard Input**. Ko boste odprli to spletno stran, bo možnost varnega vnosa podatkov vklopljena in bo delovala v skladu z nastavitvami, ki ste jih določili.

NASTAVITVE OBVESTIL O VARNOSTNIH POMANJKLJIVOSTIH V BREZŽIČNIH OMREŽJIH

Kadar ste povezani v brezžično omrežje, lahko pride do kraje vaših zaupnih podatkov, če to omrežje ni primerno zaščiteno. Kaspersky Internet Security preveri brezžična omrežja vsakič, ko se želite povezati. Če brezžično omrežje ni zaščiteno (na primer, če je uporabljen varnostno pomanjkljiv protokol šifriranja ali če je ime brezžičnega omrežja (SSID) zelo priljubljeno), bo aplikacija prikazala obvestilo, da je omrežje, s katerim se želite povezati, nezaščiteno. Kliknite na povezavo v oknu z obvestilom za informacije o varno uporabi brezžičnega omrežja.

Za nastavitev obvestil o varnostnih pomanjkljivostih brezžičnih omrežij:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu okna kliknite na povezavo z nastavitvami **(Settings)**. Pojdite v odsek **Settings**.

3. V levem delu okna izberite odsek **Protection**.

4. V desnem delu odseka **Protection** (Zaščita) izberite pododsek **Firewall** (Požarna pregrada).

   V oknu bodo prikazane nastavitve komponente požarne pregrade.

5. Izberite potrditveno polje **Notify of vulnerabilities in Wi-Fi networks,** če ni izbrano. Če ne želite prejemati obvestil, počistite potrditveno polje. V privzetem načinu je ta možnost izbrana.

6. Če je izbrana možnost **Notify of vulnerabilities in Wi-Fi networks**, lahko urejate napredne nastavitve za prikaz obvestil:

   - Izberite potrditveno polje **Block and warn about insecure transmission of passwords over the Internet**, če želite preprečiti vse prenose gesel v nešifriranem besedilnem formatu, ko na spletu vpisujete v polja za geslo (**Password**). V privzetem načinu ta možnost ni izbrana.

   - Kliknite na povezavo **Restore hidden notifications**, če želite obnoviti privzete nastavitve prikaza obvestil o prenosih gesel v nešifrirani obliki. Če ste pred tem blokirali prikaz obvestil o prenosih gesel v nešifrirani obliki, se bodo ta obvestila zdaj znova prikazovala.

ZAŠČITA FINANČNIH TRANSAKCIJ IN SPLETNIH NAKUPOV

Za zaščito zaupnih podatkov, ki jih vnašate na spletnih straneh bank in plačilnih sistemov (kot so številke bančnih kartic in gesla za dostop do storitev spletnega bančništva), ter preprečevanje kraje sredstev pri spletnih plačilih vas rešitev Kaspersky Internet Security vsakič vpraša, ali želite takšno stran odpreti v načinu zaščitenega brskalnika (Protected Browser).

Način zaščitenega brskalnika je poseben način delovanja, namenjen zaščiti vaših podatkov, ko dostopate do spletnih strani bank ali plačilnih sistemov. Zaščiteni brskalnik se zažene v ločenem okolju, da druge aplikacije ne morejo vriniti svoje kode v proces zaščitenega brskalnika.

V načinu zaščitenega brskalnika aplikacija zagotavlja zaščito pred naslednjimi vrstami groženj:

- Moduli, ki niso vredni zaupanja. Aplikacija vsakič, ko obiščete spletno stran banke ali plačilnega sistema, poišče morebitne module, ki niso vredni zaupanja.

- Orodja za prevzem nadzora nad računalnikom (rootkit). Aplikacija ob zagonu zaščitenega brskalnika poišče morebitna orodja za prevzem nadzora nad računalnikom.

- Znane varnostne pomanjkljivosti operacijskega sistema. Aplikacija ob zagonu zaščitenega brskalnika poišče morebitne pomanjkljivosti operacijskega sistema.

- Neveljavni certifikati spletnih strani bank ali plačilnih sistemov. Aplikacija preveri certifikat, ko obiščete spletno stran banke ali plačilnega sistema. Preveri, ali se certifikat nahaja v podatkovni zbirki okuženih certifikatov.

Ko odprete spletno stran v načinu zaščitenega brskalnika, se ob robovih okna brskalnika pojavi okvir. Barva okvirja ponazarja stanje zaščite.

Okvir okna brskalnika je lahko naslednjih barv:

- Zelen okvir. Pomeni, da so bila vsa preverjanja uspešna. Lahko nadaljujete z uporabo zaščitenega brskalnika.

- Rumen okvir. Pomeni, da so preverjanja odkrila varnostne težave, ki jih je treba odpraviti.

  Aplikacija lahko zazna naslednje grožnje in varnostne težave:

  - Modul, ki ni vreden zaupanja. Treba je pregledati računalnik in ga očistiti okužb.

  - Orodje za prevzem nadzora nad računalnikom (rootkit). Treba je pregledati računalnik in ga očistiti okužb.

  - Varnostna pomanjkljivost operacijskega sistema. Treba je namestiti posodobitve operacijskega sistema.

  - Neveljaven certifikat spletne strani banke ali plačilnega sistema.

Če ne odstranite odkritih groženj, varnost povezave s spletno stranjo banke ali plačilnega sistema ni zagotovljena.

Rumena barva okvirja lahko pomeni tudi, da zaščitenega brskalnika ni mogoče zagnati zaradi tehničnih omejitev. To se lahko zgodi na primer, če na vašem računalniku deluje nadzornik virtualizacije (hypervisor) drugega ponudnika ali če vaš računalnik ne podpira tehnologije virtualizacije strojne opreme.

Za pravilno delovanje zaščitenega brskalnika se prepričajte, da so vklopljeni vtičniki Safe Money. Vtičniki se samodejno vklopijo v brskalniku, ko ga ponovno zaženete prvič po namestitvi rešitve Kaspersky Internet Security. Če brskalnika niste zaprli in ga ponovno zagnali po namestitvi rešitve Kaspersky Internet Security, vtičniki niso vklopljeni.

Samodejni vklop vtičnikov ima naslednje omejitve:

- Vtičniki so vgrajeni in delujejo le v brskalnikih, ki jih podpira aplikacija.

  Vtičnike Safe Money podpirajo naslednji brskalniki:

  - Internet Explorer 8.0, 9.0, 10.0 in 11.0

    Internet Explorer 10 z uporabniškim vmesnikom Modern in Internet Explorer 11 z uporabniškim vmesnikom Modern nista podprta.

  - Mozilla Firefox 19.x, 20.x, 21.x, 22.x, 23.x, 24.x, 25.x, 26.x, 27.x, 28.x, 29.x, 30.x in 31.x.

  - Google Chrome 33.x, 34.x, 35.x in 36.x.

    Vtičniki Google Chrome niso samodejno vklopljeni, če v brskalniku ni bil ustvarjen uporabniški profil. Če želite ustvariti uporabniški profil, zapustite brskalnik in ga znova zaženite.

    Ob prvem zagonu brskalnika Google Chrome po namestitvi rešitve Kaspersky Internet Security vas spletni brskalnik pozove, da namestite razširitev z imenom Kaspersky Protection Plugin, ki vklopi vtičnike komponente Safe Money. Če ste namestitev vtičnika Kaspersky Protection Plugin zavrnili, ga lahko namestite kasneje s klikom na naslednjo povezavo: http://support.kaspersky.com/interactive/google/en/kisplugin.

- Ko posodobite svoj brskalnik, bodo vtičniki vklopljeni samodejno le v primeru, da nova različica podpira enak način vklopa vtičnikov kot prejšnja različica. Če nova različica brskalnika podpira enak način vklopa vtičnikov kot prejšnja različica, bodo vtičniki vklopljeni samodejno.

Če se vtičniki ne vklopijo samodejno, ko znova zaženete brskalnik, jih morate vklopiti ročno. Ali so vtičniki vklopljeni, lahko preverite v nastavitvah brskalnika, kjer jih lahko tudi ročno vklopite, če je to potrebno. Za več informacij o vklopu vtičnikov se lahko obrnete na sistem pomoči vašega brskalnika.

Samodejni vklop vtičnikov Safe Money lahko omogočite ali onemogočite (glej poglavje Kako omogočiti samodejni vklop vtičnikov na strani 20) v oknu z nastavitvami aplikacije.

Zaščitenega brskalnika ni mogoče zagnati, če v pododseku **Self-Defense** odseka **Additional Settings** v oknu z nastavitvami aplikacij ni izbrano potrditveno polje **Enable Self-Defense**.

V TEM POGLAVJU

UREJANJE NASTAVITEV KOMPONENTE SAFE MONEY

Če želite urejati nastavitve komponente Safe Money:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo **Settings**, da se odpre odsek z nastavitvami **Settings**.
3. V levem delu okna izberite odsek **Protection**.
4. V desnem delu odseka **Protection** izberite pododsek **Safe Money**.

   V oknu bodo prikazane nastavitve komponente Safe Money.
5. Vklopite komponento Safe Money, tako da kliknete na stikalo v zgornjem delu okna.
6. Če želite vklopiti obvestila glede varnostnih pomanjkljivosti, ki so bile odkrite v operacijskem sistemu, pred zagonom zaščitenega brskalnika izberite potrditveno polje **Notify about operating system vulnerabilities**.

UREJANJE NASTAVITEV KOMPONENTE SAFE MONEY ZA DOLOČENO SPLETNO STRAN

Če želite urediti nastavitve komponente Safe Money za določeno spletno stran:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite gumb **Safe Money**.

   Odpre se okno **Safe Money**.
3. Kliknite gumb **Add website to Safe Money**.

   V desnem delu okna bodo prikazana polja za vnos podatkov o spletni strani.
4. V polje **Website for Safe Money** vnesite naslov spletne strani, ki jo želite odpreti v zaščitenem brskalniku.

   Spletni naslov mora vsebovati predpono za protokol https://, ki jo privzeto uporablja zaščiteni brskalnik.
5. Če je potrebno, v polje **Description** vpišite ime ali opis spletne strani.
6. Izberite dejanje, za katerega želite, da ga zaščiteni brskalnik izvede, ko odprete spletno stran:

- Če želite, da se spletna stran odpre v zaščitenem brskalniku vsakič, ko jo obiščete, izberite **Run Protected Browser**.
- Če želite, da vas Kaspersky Internet Security pozove k dejanju, ko je spletna stran odprta, izberite **Prompt for action**.
- Če želite za spletno stran izklopiti komponento Safe Money, izberite možnost **Do not run Protected Browser**.

7. V desnem delu okna kliknite gumb **Add**.

Spletna stran bo prikazana na seznamu v levem delu okna.

KAKO OMOGOČITI SAMODEJNI VKLOP VTIČNIKOV SAFE MONEY

Če želite omogočiti vklop vtičnikov Safe Money v brskalnikih:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo **Settings**, da se odpre odsek z nastavitvami **Settings**.
3. V levem delu okna izberite odsek **Protection**.
4. V desnem delu odseka **Protection** izberite odsek **Web Anti-Virus**.
5. V oknu z nastavitvami **Web Anti-Virus**, ki se odpre, kliknite na povezavo **Advanced Settings**, da se odpre okno **Advanced settings of Web Anti-Virus**.
6. V odseku **Web browser extensions** izberite potrditveno polje **Automatically activate application plug-ins in all web browsers**.

O ZAŠČITI PRED POSNETKI ZASLONA

Da bo zaščitila vaše podatke, ko brskate po zaščitenih straneh, rešitev Kaspersky Internet Security preprečuje vohunskim programom, da bi delali nepooblaščene posnetke zaslona. Zaščita pred posnetki zaslona je v privzetem načinu že vklopljena. Če je bila zaščita izklopljena ročno, jo lahko znova vklopite v oknu z nastavitvami aplikacije (glej poglavje Kako vklopiti zaščito pred posnetki zaslona na strani 20).

Rešitev Kaspersky Internet Security uporablja tehnologijo nadzornika virtualizacije (hypervisor), ki zagotavlja zaščito pred posnetki zaslona. Na računalnikih z operacijskim sistemom Microsoft Windows 8 x64 ima zaščita pred posnetki zaslona, ki jo nudi nadzornik rešitve Kaspersky Internet Security, naslednje omejitve:

- Ta možnost ni na voljo, ko je zagnan nadzornik virtualizacije drugega ponudnika, kot na primer VMware. Ko boste zaprli nadzornika drugega ponudnika, bo zaščita proti posnetkom zaslona znova na voljo.
- Ta možnost ni na voljo, če procesor vašega računalnika ne podpira tehnologije za virtualizacijo strojne opreme. Več informacij o tem, ali vaš procesor podpira virtualizacijo strojne opreme, poiščite v dokumentaciji, ki ste jo prejeli skupaj z računalnikom, ali na spletni strani proizvajalca procesorja.
- Ta možnost ni na voljo, če ob zagonu zaščitenega brskalnika deluje nadzornik drugega ponudnika (kot na primer nadzornik VMware).

KAKO VKLOPITI ZAŠČITO PRED POSNETKI ZASLONA

Če želite vklopiti zaščito pred posnetki zaslona:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu okna kliknite na povezavo z nastavitvami **(Settings)**. Pojdite v odsek **Settings**.
3. V levem delu okna izberite odsek **Protection**.

4. V desnem delu odseka **Protection** izberite pododsek **Safe Money** in se prepričajte, da je stikalo Safe Money vklopljeno.

   Odpre se okno z nastavitvami **Safe Money.**

8. V odseku **Additional** izberite potrditveno polje **Block capturing screenshots in Protected Browser**.

O ZAŠČITI PODATKOV V ODLOŽIŠČU

Rešitev Kaspersky Internet Security aplikacijam onemogoča nepooblaščen dostop do odložišča, ko izvajate spletna plačila, in tako kriminalcem preprečuje krajo podatkov. Takšno onemogočanje dostopa deluje le, če aplikacija, ki ni vredna zaupanja, poskuša nepooblaščeno dostopati do vašega odložišča. Če ročno kopirate podatke iz okna aplikacije v okno druge aplikacije (na primer iz aplikacije Notepad v okno brskalnika), je dostop do odložišča dovoljen.

PREVERJANJE, ALI JE SPLETNA STRAN VARNA

Preden kliknete na povezavo do spletne strani, lahko z rešitvijo Kaspersky Internet Security preverite, ali je spletna stran varna, in sicer s pomočjo možnosti Kaspersky URL Advisor, ki je vgrajena v komponento za protivirusno zaščito na spletu.

Kaspersky URL Advisor ni na voljo z brskalnikom Microsoft Internet Explorer 10 in 11 z uporabniškim vmesnikom Modern.

Kaspersky URL Advisor je integriran v brskalnike Microsoft Internet Explorer, Google Chrome in Mozilla Firefox ter preverja povezave na spletnih straneh, naloženih v brskalniku. Rešitev Kaspersky Internet Security ob vsaki povezavi prikaže eno od naslednjih ikon:

-  – če Kaspersky Lab ocenjuje, da je povezana spletna stran varna
-  – če ni informacij o varnostnem stanju povezane spletne strani
-  – če Kaspersky Lab ocenjuje, da je povezana spletna stran nevarna

Za ogled okna z več podrobnostmi o povezavi, se z miško premaknite nad ustrezno ikono.

V privzetem načinu rešitev Kaspersky Internet Security preverja le povezave med rezultati iskanja. Lahko pa vklopite preverjanje povezav na vseh spletnih straneh.

➡ *Če želite vklopiti preverjanje povezav na spletnih straneh:*

1. Odprite glavno okno aplikacije.

2. V spodnjem delu glavnega okna kliknite na povezavo **Settings**, da se odpre okno z nastavitvami **Settings**.

3. V odseku **Protection** izberite pododsek **Web Anti-Virus**.

   V oknu bodo prikazane nastavitve za komponento protivirusne zaščite na spletu.

4. V spodnjem delu okna kliknite na povezavo **Advanced Settings**. Odprlo se bo okno z naprednimi nastavitvami komponente protivirusne zaščite na spletu.

5. V odseku **Kaspersky URL Advisor** izberite potrditveno polje **Check URLs**.

6. Če želite, da komponenta za protivirusno zaščito na spletu preverja vsebino vseh spletnih strani, izberite možnost **On all websites except those specified**.

   Če je potrebno, določite spletna mesta, ki jim zaupate, tako da kliknete na povezavo **Configure exclusions**. Komponenta za protivirusno zaščito na spletu ne bo preverjala vsebine navedenih spletnih strani ali šifriranih povezav z navedenimi spletnimi stranmi.

7. Če želite, da komponenta za protivirusno zaščito na spletu preverja le vsebino določenih spletnih strani:

   a. Izberite možnost **On specified websites only**.

   b. Kliknite na povezavo **Configure checked websites**.

   c. V oknu **Configure checked websites**, ki se odpre, kliknite gumb **Add**.

   d. V oknu **Add URL**, ki se odpre, vnesite naslov URL spletne strani, katere vsebino želite preveriti.

   e. Izberite stanje preverjanja za spletno stran (če je stanje *Active*, bo komponenta za protivirusno zaščito na spletu preverjala vsebino spletne strani).

   f. Kliknite gumb **Add**.

      Navedena spletna stran se bo pojavila na seznamu preverjenih spletnih strani v oknu **Checked websites**. Komponenta za protivirusno zaščito na spletu preverja naslove URL na tej spletni strani.

8. Če želite urejati napredne nastavitve za preverjanje naslovov URL, v oknu **Advanced settings of Web Anti-Virus** v odseku **Kaspersky URL Advisor** kliknite na povezavo **Configure Kaspersky URL Advisor**.

   Odpre se okno **Configure Kaspersky URL Advisor**.

9. Če želite, da vas komponenta za protivirusno zaščito na spletu obvešča o varnosti povezav na vseh spletnih straneh, v odseku **Check URLs** izberite možnost **All URLs**.

10. Če želite, da komponenta za protivirusno zaščito na spletu prikaže informacije o tem, ali povezava pripada določeni kategoriji spletnih vsebin, kot na primer žaljivo, obsceno (*Profanity, obscenity*):

    a. Izberite potrditveno polje **Show information on the categories of website content**.

    b. Izberite kategorije spletnih vsebin, za katere želite, da se v komentarjih prikazujejo informacije.

Komponenta za protivirusno zaščito na spletu preverja povezave do navedenih spletnih strani in prikazuje informacije o kategorijah povezav v skladu s trenutnimi nastavitvami.

ODSTRANJEVANJE SLEDI AKTIVNOSTI NA RAČUNALNIKU IN INTERNETU

Uporabniške aktivnosti na računalniku se zabeležijo v operacijskem sistemu. Shranjujejo se naslednje informacije:

- Podrobnosti o iskanih ključnih besedah in obiskanih spletnih straneh
- Informacije o uporabljenih aplikacijah in odprtih ter shranjenih datotekah
- Zapisi v dnevniku sistema Windows
- Druge informacije o aktivnostih uporabnikov

Napadalci in nepooblaščeni uporabniki lahko pridobijo dostop do zasebnih informacij o preteklih aktivnostih uporabnika računalnika.

Kaspersky Internet Security vključuje čarovnika za čiščenje zasebnih podatkov (Privacy Cleaner Wizard), ki odstrani sledi uporabniških aktivnosti iz operacijskega sistema.

Koraki za zagon čarovnika:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo **Show Additional Tools** za prikaz dodatnih orodij. Odpre se okno z orodji **(Tools)**.
3. V levem delu okna **Tools** kliknite na povezavo **Privacy Cleaner**, da zaženete čarovnika za odstranjevanje zasebnih podatkov.

Čarovnik vsebuje več strani (korakov), po katerih se lahko premikate s klikanjem gumbov **Back** (nazaj) in **Next** (naprej). Če želite zapreti čarovnika, ko svoje delo opravi, kliknite gumb **Finish**. Čarovnika lahko kadarkoli zaustavite s klikom gumba **Cancel**.

Oglejmo si korake čarovnika bolj podrobno.

1. korak. Zagon čarovnika

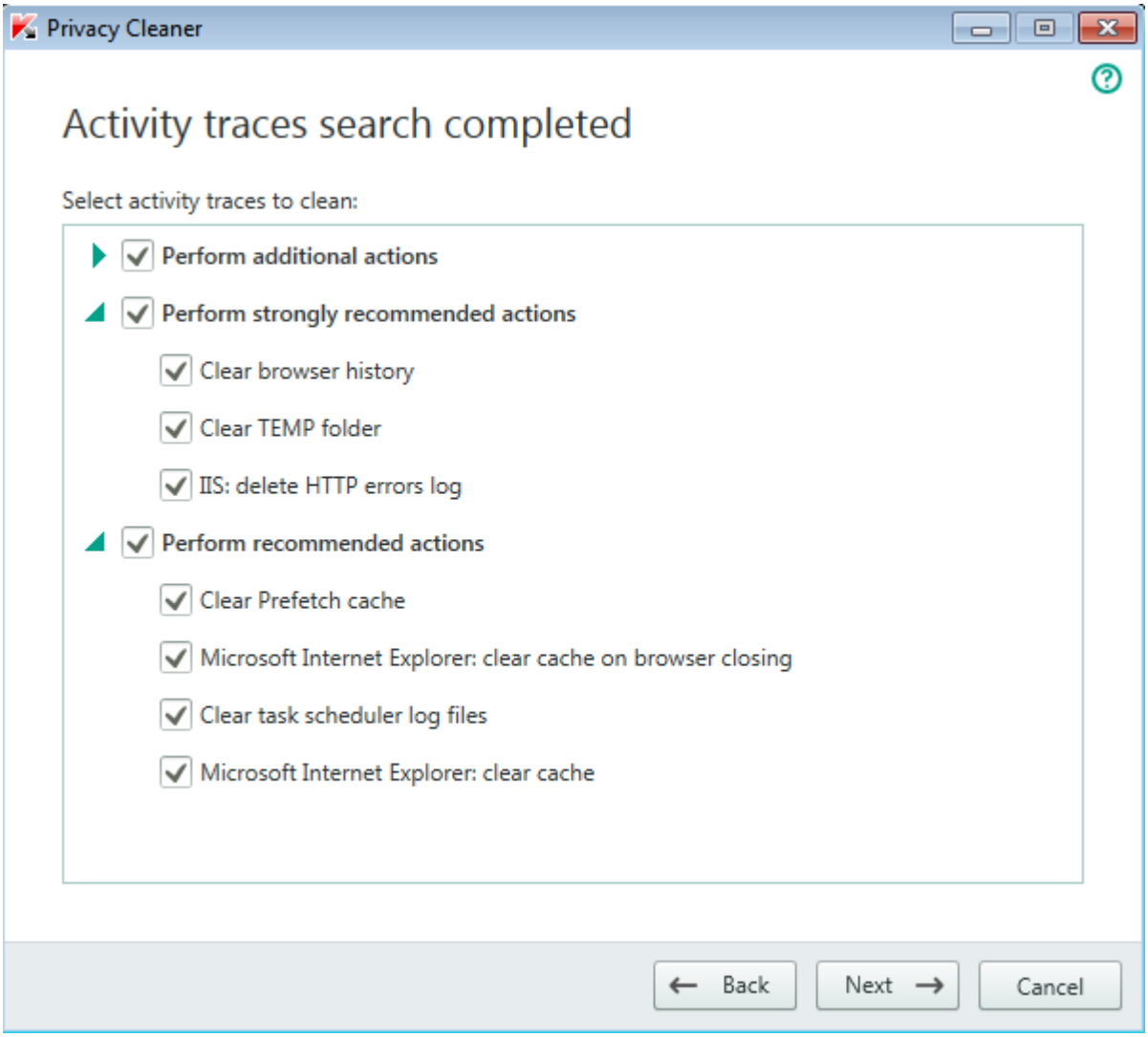
Prepričajte se, da je možnost **Search for user activity traces** izbrana. Kliknite gumb **Next** za zagon čarovnika.

2. korak. Iskanje sledi aktivnosti

Čarovnik poišče sledi aktivnosti na vašem računalniku. Iskanje lahko traja nekaj časa. Ko je iskanje zaključeno, čarovnik samodejno nadaljuje z naslednjim korakom.

3. korak. Izbira ukrepov čarovnika za odstranjevanje zasebnih podatkov

Ko je iskanje zaključeno, vas čarovnik obvesti o odkritih sledeh aktivnosti in vas vpraša, katere ukrepe naj izvede, da odstrani te sledi (glej spodnjo sliko).



Slika 4. Odkrite sledi aktivnosti in priporočila, kako jih odstraniti

Za pregled ukrepov v skupini kliknite na ikono ▸ na levi strani imena skupine.

Za ukrepe, ki jih želite izvesti, izberite potrditveno polje na levi strani ustreznega opisa ukrepa. Privzeto čarovnik izvede vse priporočene in močno priporočene ukrepe. Če določenega ukrepa ne želite izvesti, počistite potrditveno polje ob njegovem opisu.

Odstranjevanje ukrepov, ki so izbrani privzeto, ni priporočeno. Lahko namreč ogrozi varnost vašega računalnika.

Ko izberete ukrepe, kliknite gumb za naprej (**Next**).

4. korak. Brisanje sledi aktivnosti

Čarovnik bo izvedel ukrepe, ki ste jih izbrali v prejšnjem koraku. Brisanje sledi aktivnosti lahko traja nekaj časa. Za brisanje nekaterih sledi aktivnosti bo morda treba ponovno zagnati računalnik; v takšnem primeru vas bo čarovnik o tem obvestil.

Ko je čiščenje končano, čarovnik samodejno nadaljuje z naslednjim korakom.

5. korak. Zaključek čarovnika

Kliknite gumb **Finish**, s čimer zaprete čarovnika.

NADZOR UPORABNIŠKIH AKTIVNOSTI NA RAČUNALNIKU IN INTERNETU

This section provides information about how to control users' actions on the computer and on the Internet by using Kaspersky Internet Security.

IN THIS SECTION

UPORABA STARŠEVSKEGA NADZORA

Starševski nadzor omogoča spremljanje aktivnosti, ki jih izvajajo uporabniki na lokalnem računalniku in na spletu. Uporabite ga lahko za omejitev dostopa do internetnih virov in aplikacij, kakor tudi za ogled poročil o aktivnostih uporabnikov.

Vse več otrok in najstnikov ima dostop do računalnikov in spletnih virov. Uporaba računalnikov in interneta predstavlja številne izzive in tveganja za otroke:

- Izguba časa in/ali denarja z obiskom klepetalnic, igranjem iger, obiskovanjem spletnih trgovin ali sodelovanjem na dražbah
- Dostop do spletnih strani, namenjenih odraslemu občinstvu, kot so strani, posvečene pornografiji, ekstremističnim vsebinam, orožju, drogam ali nasilju
- Prenos datotek, okuženih s škodljivo programsko opremo
- Zdravstvene težave, ki jih povzroči pretirana uporaba računalnika
- Stiki s tujci, ki se morda pretvarjajo, da so njihovi vrstniki, da bi pridobili osebne informacije o nepolnoletnih uporabnikih, kot so njihovo ime, fizični naslov ali ura, ko ni nikogar doma

Starševski nadzor vam omogoča, da zmanjšate tveganja, ki jih prinaša uporaba računalnikov in interneta. To omogočajo naslednje funkcije:

- Omejitev časa za uporabo računalnika in interneta.
- Priprava seznamov dovoljenih in prepovedanih iger in aplikacij ter začasna prepoved uporabe dovoljenih aplikacij.

- Priprava seznamov dovoljenih in blokiranih spletnih strani ter izbira kategorij prepovedanih strani z neprimernimi vsebinami.
- Vklop varnega načina iskanja v iskalnikih (povezave do spletnih strani z neprimernimi vsebinami niso prikazane med rezultati iskanja).
- Omejitev prenosa datotek z interneta.
- Priprava seznamov stikov, ki so dovoljeni ali blokirani v odjemalcih za takojšnje sporočanje in družabnih omrežjih.
- Ogled zgodovine sporočil, poslanih prek odjemalcev za takojšnje sporočanje in družabnih omrežij.
- Preprečitev pošiljanja nekaterih osebnih podatkov.
- Iskanje določenih ključnih besed v zgodovini sporočil.

Nastavitve starševskega nadzora lahko urejate za vsak uporabniški račun na računalniku posebej. Prav tako si lahko ogledujete poročila komponente starševskega nadzora o aktivnostih nadzorovanih uporabnikov.

KAKO DO NASTAVITEV STARŠEVSKEGA NADZORA

Za dostop do nastavitev starševskega nadzora:

1. Odprite glavno okno aplikacije.
2. V glavnem oknu aplikacije kliknite gumb **Parental Control** (starševski nadzor).
3. Ko prvič odprete okno **Parental Control**, vas aplikacije pozove, da nastavite geslo za zaščito nastavitev starševskega nadzora. Izberite eno od naslednjih možnosti:
   - Če želite dostop do nastavitev starševskega nadzora zaščititi z geslom, izpolnite polji **Password** (geslo) in **Confirm** (potrdi) ter za nadaljevanje kliknite gumb **Continue**.
   - Če dostopa do nastavitev starševskega nadzora ne želite zaščititi z geslom, kliknite na povezavo **Skip**, da odprete nastavitve starševskega nadzora.

   Odprlo se bo okno **Parental Control**.
4. Izberite uporabniški račun in kliknite na povezavo **Configure restrictions**, da se odpre okno z nastavitvami starševskega nadzora.

KAKO NADZOROVATI UPORABO RAČUNALNIKA

Starševski nadzor vam omogoča, da omejite količino časa, ki ga uporabnik prebije za računalnikom. Določite lahko časovni interval, v katerem želite, da starševski nadzor onemogoči dostop do računalnika (čas za spanje), kakor tudi dnevno omejitev skupne uporabe računalnika. Nastavite lahko različne omejitve za delovne dni in konec tedna.

Če želite nastaviti časovne omejitve uporabe računalnika:

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).
2. V oknu z nastavitvami starševskega nadzora izberite odsek **Computer**.
3. Če želite določiti časovni interval, v katerem bo starševski nadzor onemogočal dostop do računalnika, v odsekih **Weekdays** (delovni dnevi) in **Weekends** (konec tedna) izberite potrditveno polje **Block access from**.
4. V spustnem seznamu poleg možnosti **Block access from** določite čas začetka intervala.

5. V spustnem seznamu poleg možnosti **to** določite čas konca intervala.

   Urnik uporabe računalnika lahko nastavite tudi z uporabo tabele. Za ogled tabele kliknite gumb  .

   Starševski nadzor uporabniku onemogoči dostop do računalnika v izbranem časovnem intervalu.

6. Če želite nastaviti časovno omejitev dnevne uporabe računalnika, v odsekih **Weekdays** (delovni dnevi) in **Weekends** (konec tedna) izberite potrditveno polje **Allow access for no longer than** in na spustnem seznamu poleg potrditvenega polja izberite želeni časovni interval.

   Ko je ta dnevna časovna omejitev prekoračena, starševski nadzor uporabniku onemogoči nadaljnji dostop do računalnika.

7. Če želite nastaviti premore v uporabi računalnika za posameznega uporabnika, v odseku **Time breaks** izberite potrditveno polje **Take a break every** in nato na spustnem seznamu poleg potrditvenega polja izberite vrednosti za pogostost premorov (na primer vsako uro) in njihovo trajanje (na primer 10 minut).

8. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Starševski nadzor bo uporabniku onemogočil dostop do računalnika v skladu z novimi nastavitvami.

NADZOR UPORABE INTERNETA

Z uporabo starševskega nadzora lahko omejite čas, preživet na internetu, in uporabnikom preprečite dostop do določenih kategorij spletnih strani ali točno določenih spletnih strani. Prav tako lahko uporabnikom preprečite prenos določenih vrst datotek (kot so arhivi ali video posnetki) z interneta.

- *Če želite nastaviti časovno omejitev za uporabo interneta:*

  1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

  2. V oknu z nastavitvami starševskega nadzora izberite odsek **Internet**.

  3. Če želite omejiti skupni čas uporabe interneta na delovne dni, v odseku **Internet access restriction** izberite potrditveno polje **Limit access on weekdays to <HH:MM> hours per day** in nato na spustnem seznamu poleg potrditvenega polja izberite vrednost časovne omejitve.

  4. Če želite omejiti skupni čas uporabe interneta ob koncu tedna, izberite potrditveno polje **Limit access on weekends to <HH:MM> hours per day** in nato na spustnem seznamu poleg potrditvenega polja izberite vrednost časovne omejitve.

  5. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

  Starševski nadzor bo omejil količino časa, ki ga lahko uporabnik preživi na internetu, v skladu z vrednostmi, ki ste jih določili.

- *Če želite omejiti dostop do določenih spletnih strani:*

  1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

  2. V oknu z nastavitvami starševskega nadzora izberite odsek **Internet**.

  3. Če želite preprečiti prikaz vsebin za odrasle v rezultatih iskanja, v odseku **Control Web Browsing** izberite potrditveno polje **Enable Safe Search**.

     Ko boste iskali informacije na spletnih straneh, kot so Google, YouTube (velja le za uporabnike, ki se niso prijavili na spletno stran youtube.com z lastnim računom), Bing, Yahoo!, Mail.ru, VKontakte in Yandex, med rezultati iskanja ne bodo prikazane vsebine za odrasle.

4. Če želite onemogočiti dostop do spletnih strani, ki pripadajo določenim kategorijam:

   a. V odseku **Control Web Browsing** izberite potrditveno polje **Block access to the following websites**.

   b. Izberite **Adult websites** in kliknite na povezavo **Select categories of websites**, da se odpre okno z naslovom **Block access to website categories**.

   c. Izberite potrditvena polja poleg kategorij spletnih strani, do katerih želite onemogočiti dostop.

      Starševski nadzor bo preprečil vse poskuse uporabnika, da bi odprl spletno stran, če so na njej vsebine, ki sodijo v katero od blokiranih kategorij.

5. Če želite onemogočiti dostop do točno določenih spletnih strani:

   a. V odseku **Control Web Browsing** izberite potrditveno polje **Block access to the following websites**.

   b. Izberite **All websites except for exclusions allowed in the list** in kliknite na povezavo **Add exclusions**, da se odpre okno z izjemami (**Exclusions**).

   c. V spodnjem delu okna kliknite gumb **Add**.

      Odpre se okno **Add new website**.

   d. Vpišite naslov spletne strani, do katere želite preprečiti dostop, tako da izpolnite polje **Web address**.

   e. V odseku **Scope** določite, kaj vse želite blokirati: celotno spletno mesto ali le določeno stran.

   f. Če želite onemogočiti dostop do določene spletne strani, v odseku **Action** izberite **Block**.

   g. Kliknite gumb **Add**.

   Določena spletna stran se bo pojavila na seznamu v oknu **Exclusions**.

6. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Starševski nadzor bo preprečil vse poskuse uporabnika, da bi odprl navedeno spletno stran, v skladu s trenutnimi nastavitvami.

- *Če želite prepovedati prenos določenih vrst datotek z interneta:*

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

2. V oknu z nastavitvami starševskega nadzora izberite odsek **Internet**.

3. V odseku **Limit file downloading** izberite potrditvena polja poleg vrst datotek, katerih prenos želite preprečiti.

4. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Starševski nadzor bo onemogočil prenos datotek navedenih vrst z interneta.

NADZOR ZAGONA IGER IN APLIKACIJ

Z uporabo starševskega nadzora lahko uporabniku dovolite ali prepoveste zagon iger glede na to, ali so primerne za njegovo starost. Prav tako lahko uporabniku onemogočite zagon določenih aplikacij (kot so igre ali odjemalci takojšnjega sporočanja) ali omejite čas uporabe aplikacij.

- *Če želite preprečiti zagon iger s starostno neprimernimi vsebinami:*

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

2. V oknu z nastavitvami starševskega nadzora izberite odsek **Applications**.

3. V odseku **Block games by content** onemogočite zagon iger, ki so neprimerne za izbranega uporabnika glede na njegovo starost in/ali vsebino:

   a. Če želite blokirati vse igre z vsebino, neprimerno za starost uporabnika, izberite potrditveno polje **Block games by age rating** in v spustnem seznamu poleg potrditvenega polja izberite starostno omejitev.

   b. Če želite blokirati igre z vsebinami, ki pripadajo določeni kategoriji:

      a. Izberite potrditveno polje **Block games from adult categories**.

      b. Kliknite na povezavo Select categories of games, da se odpre okno **Block games by categories**.

      c. Izberite potrditvena polja poleg kategorij vsebin, ki ustrezajo igram, katere želite blokirati.

4. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Če želite omejiti zagon točno določene aplikacije:

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

2. V oknu z nastavitvami starševskega nadzora izberite odsek **Applications**.

3. V spodnjem delu okna kliknite na povezavo **Add application to list**, da se odpre pogovorno okno **Open**, in izberite izvršno datoteko aplikacije.

   Izbrana aplikacija se bo pojavila na seznamu v odseku **Block specified applications**. Kaspersky Internet Security samodejno doda aplikacijo določeni kategoriji, na primer igram (*Games*).

4. Če želite blokirati aplikacijo, izberite potrditveno polje poleg imena aplikacije na seznamu. Prav tako lahko blokirate vse aplikacije, ki pripadajo določeni kategoriji, tako da izberete potrditveno polje poleg imena te kategorije na seznamu (na primer, blokirate lahko kategorijo *Games*).

5. Če želite omejiti čas uporabe aplikacije, izberite aplikacijo ali kategorijo aplikacij na seznamu in kliknite na povezavo **Configure rules**, da se odpre okno **Application usage restriction**.

6. Če želite določiti časovno omejitev uporabe aplikacije na delovne dni in ob koncu tedna, v odsekih **Weekdays** (delovni dnevi) in **Weekends** (konec tedna) izberite potrditveno polje **Allow access for no longer than** ter na spustnem seznamu določite, koliko ur na dan lahko uporabnik uporablja aplikacijo. Prav tako lahko z uporabo tabele določite čas, ko želite uporabniku dovoliti/prepovedati uporabo aplikacije. Za ogled tabele kliknite gumb  .

7. Če želite nastaviti premore v uporabi aplikacije, v odseku **Time breaks** izberite potrditveno polje **Take a break every** in na spustnem seznamu izberite vrednosti za pogostost in dolžino premorov.

8. Kliknite gumb **Save**.

9. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Ko bo uporabnik odprl aplikacijo, bo starševski nadzor upošteval nastavljene omejitve.

NADZOR SPOROČANJA PREKO DRUŽABNIH OMREŽIJ

Z uporabo starševskega nadzora si lahko ogledate sporočila uporabnika, poslana prek družabnih omrežij in odjemalcev takojšnjega sporočanja, obenem pa lahko onemogočite izmenjavo sporočil z določenimi stiki.

Če želite nastaviti nadzor nad uporabnikovimi sporočili:

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).
2. V oknu z nastavitvami starševskega nadzora izberite odsek **Communication**.
3. Če si želite ogledati zgodovino sporočil in po potrebi blokirati določene stike:
   a. Izberite možnost **Block messaging with all contacts except contacts that are allowed**.
   b. Kliknite na povezavo **Contacts**, da se odpre okno **Contacts** (stiki).
   c. Ogledate si lahko stike, s katerimi si je uporabnik dopisoval. Določene uporabnike lahko prikažete v oknu z uporabo ene od naslednjih metod:
      - Če si želite ogledati zgodovino uporabnikovih sporočil, poslanih preko določenega družabnega omrežja ali odjemalca takojšnjega sporočanja, na levi strani okna na spustnem seznamu izberite želeno možnost.
      - Če si želite ogledati stike, s katerimi si je uporabnik največ dopisoval, na spustnem seznamu na desni strani okna izberite možnost **By number of messages**.
      - Če si želite ogledati stike, s katerimi si je uporabnik dopisoval na določen dan, na spustnem seznamu na desni strani okna izberite možnost **By date of messaging**.
   d. Če si želite ogledati uporabnikova sporočila, izmenjana z določenim stikom, kliknite na stik na seznamu.

      Odpre se okno **Messaging log** z zgodovino sporočil.
   e. Če želite onemogočiti izmenjavo sporočil med uporabnikom in izbranim stikom, kliknite gumb **Block**.
4. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Starševski nadzor bo preprečil izmenjavo sporočil med uporabnikom in izbranim stikom.

NADZOR VSEBINE SPOROČIL

Z uporabo starševskega nadzora lahko spremljate in preprečite uporabnikove poskuse, da bi v sporočila dodal določene osebne podatke (kot so imena, telefonske številke, številke bančnih kartic) in ključne besede (kot so nespodobne besede).

Če želite nastaviti nadzor nad prenosom osebnih podatkov:

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).
2. V oknu z nastavitvami starševskega nadzora izberite odsek **Content Control**.
3. V odseku **Private data transfer control** izberite potrditveno polje **Block private data transfer to third parties**.
4. Kliknite na povezavo **Edit list of private data**, da se odpre okno **Private data list**.
5. V spodnjem delu okna kliknite gumb **Add**.

   Odpre se okno, kamor lahko dodate zasebne podatke.
6. Izberite vrsto zasebnih podatkov (na primer telefonska številka - "phone number"), tako da kliknete na ustrezno povezavo, ali pa vnesite opis v polje **Field name**.
7. V polju **Value** določite zasebne podatke (kot so vaš priimek ali telefonska številka).

8. Kliknite gumb **Add**.

   Zasebni podatki so navedeni v oknu **Private data list**.

9. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Starševski nadzor bo spremljal in preprečil vsak poskus uporabnika, da bi uporabil navedene zasebne podatke med pošiljanjem sporočil prek odjemalcev takojšnjega sporočanja in na spletnih straneh.

Če želite nastaviti nadzor nad ključnimi besedami za sporočila:

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

2. V oknu z nastavitvami starševskega nadzora izberite odsek **Content Control**.

3. V odseku **Keyword Control** izberite potrditveno polje **Enable Keyword Control**.

4. Kliknite na povezavo **Edit list of key words**, da se odpre okno **Keyword Control**.

5. V spodnjem delu okna kliknite gumb **Add**.

   Odpre se okno, kamor lahko dodate ključno besedo.

6. Vnesite ključno besedno zvezo v polje **Value** in kliknite gumb **Add**.

   Izbrana ključna besedna zveza se bo pojavila na seznamu v oknu **Keyword Control**.

7. V oknu **Parental Control** vklopite stikalo **Parental Control**, ki se nahaja poleg uporabniškega računa.

Starševski nadzor bo preprečil prenos sporočil, ki vsebujejo izbrano ključno besedno zvezo, tako pri pošiljanju sporočil prek interneta kot v odjemalcih takojšnjega sporočanja.

OGLED POROČILA O AKTIVNOSTIH UPORABNIKA

Dostopate lahko do poročil o aktivnostih vsakega uporabniškega računa, za katerega je vklopljen starševski nadzor, z ločenim poročanjem o vsaki kategoriji nadzorovanih dogodkov.

Če si želite ogledati poročilo o aktivnostih nadzorovanega uporabniškega računa:

1. Odprite okno z nastavitvami starševskega nadzora (glej poglavje Kako do nastavitev starševskega nadzora na strani 27).

2. Izberite uporabniški račun in kliknite na povezavo **View report**, da se odpre okno s poročili.

3. V odseku z ustrezno vrsto omejitve (na primer **Internet** ali **Communication** (komunikacija)) odprite poročilo o nadzorovanih aktivnostih, tako da kliknete na povezavo **Details**.

V oknu bo prikazano poročilo o nadzorovanih aktivnostih uporabnika.

KAKO Z GESLOM ZAŠČITITI DOSTOP DO UPRAVLJAVSKIH MOŽNOSTI REŠITVE KASPERSKY INTERNET SECURITY

Isti računalnik lahko uporablja več uporabnikov, ki so različno izkušeni ali izobraženi o uporabi računalnika. Neomejen dostop različnih uporabnikov do rešitve Kaspersky Internet Security in njenih nastavitev lahko predstavlja grožnjo varnosti računalnika.

Za omejitev dostopa do aplikacije lahko nastavite administratorsko geslo in določite, katere aktivnosti zahtevajo vpis tega gesla:

- spreminjanje nastavitev aplikacije,
- zapiranje aplikacije,
- odstranitev aplikacije.

Če želite nadzor nad aplikacijo Kaspersky Internet Security zaščititi z geslom:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo **Settings**, da se odpre odsek z nastavitvami **Settings**.
3. V levem delu okna izberite odsek **General** in kliknite na povezavo **Set up password protection**, da se odpre okno **Password protection**.
4. V oknu, ki se odpre, izpolnite polji **New password** (novo geslo) in **Confirm password** (potrdi geslo).
5. V skupini nastavitev **Password scope** določite aktivnosti aplikacije, do katerih želite omejiti dostop.

Pozabljenega gesla ne morete ponovno pridobiti. Če ste pozabili svoje geslo, se morate za dostop do nastavitev rešitve Kaspersky Internet Security obrniti na tehnično podporo.

Kako začasno zaustaviti in ponovno nastaviti zaščito računalnika

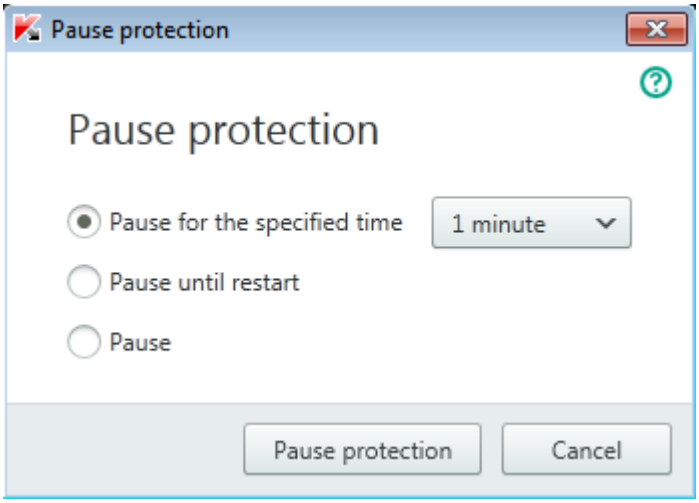
Začasna zaustavitev pomeni, da za nekaj časa izklopite vse komponente zaščite.

Ko je zaščita začasno zaustavljena ali Kaspersky Internet Security ne deluje, so aktivnosti aplikacij, ki delujejo na vašem računalniku, nadzorovane. Informacije o rezultatih nadzora aktivnosti aplikacij so shranjene v operacijskem sistemu. Ko rešitev Kaspersky Internet Security znova zaženete ali ponovno vklopite zaščito, Kaspersky Internet Security uporabi te informacije, da zaščiti vaš računalnik pred škodljivimi aktivnostmi, ki so bile morda izvedene, ko je bila zaščita začasno zaustavljena ali rešitev Kaspersky Internet Security ni delovala. Informacije o rezultatih nadzora aktivnosti aplikacij so shranjene za nedoločen čas. Te informacije so izbrisane, če je rešitev Kaspersky Internet Security odstranjena z vašega računalnika.

- *Če želite začasno zaustaviti zaščito svojega računalnika:*

1. Iz priročnega menija ikone aplikacije v območju za obvestila opravilne vrstice izberite možnost za začasno zaustavitev zaščite (**Pause protection**).

   Odpre se okno **Pause protection** (glej spodnjo sliko).



Slika 6. Okno za začasno zaustavitev zaščite

2. V oknu **Pause protection** izberite časovni interval, po katerem želite, da se zaščita znova vklopi:

   - **Pause for the specified time –** zaščita se vklopi po preteku časovnega intervala, ki ste ga izbrali na spustnem seznamu.
   - **Pause until restart –** zaščita se vklopi po tem, ko ponovno zaženete aplikacijo ali operacijski sistem (če se aplikacija zažene samodejno ob zagonu sistema).
   - **Pause** – zaščita se vklopi, ko to želite vi.

- *Če želite ponovno vklopiti zaščito računalnika:*

  Iz priročnega menija ikone aplikacije v območju za obvestila opravilne vrstice izberite možnost za ponovni vklop zaščite (**Resume protection**).

KAKO ZOPET VZPOSTAVITI PRIVZETE NASTAVITVE APLIKACIJE

Kadarkoli lahko znova vzpostavite priporočene nastavitve podjetja Kaspersky Lab za rešitev Kaspersky Internet Security. Nastavitve lahko ponovno vzpostavite z uporabo *čarovnika za konfiguracijo aplikacije.*

Ko čarovnik zaključi operacijo, je za vse komponente zaščite nastavljena priporočena (*Recommended*) raven zaščite. Ko znova vzpostavite priporočeno raven zaščite, lahko shranite vrednosti predhodno določenih nastavitev za komponente aplikacije.

- *Če želite zagnati čarovnika za konfiguracijo aplikacije:*

  1. Odprite glavno okno aplikacije.
  2. V spodnjem delu okna kliknite na povezavo z nastavitvami **(Settings)**.

     V oknu se prikaže odsek **Settings**.
  3. Izberite odsek **General**.

     V oknu se prikažejo nastavitve aplikacije Kaspersky Internet Security.
  4. V spodnjem delu okna na spustnem seznamu **Manage Settings** izberite možnost **Restore settings**.

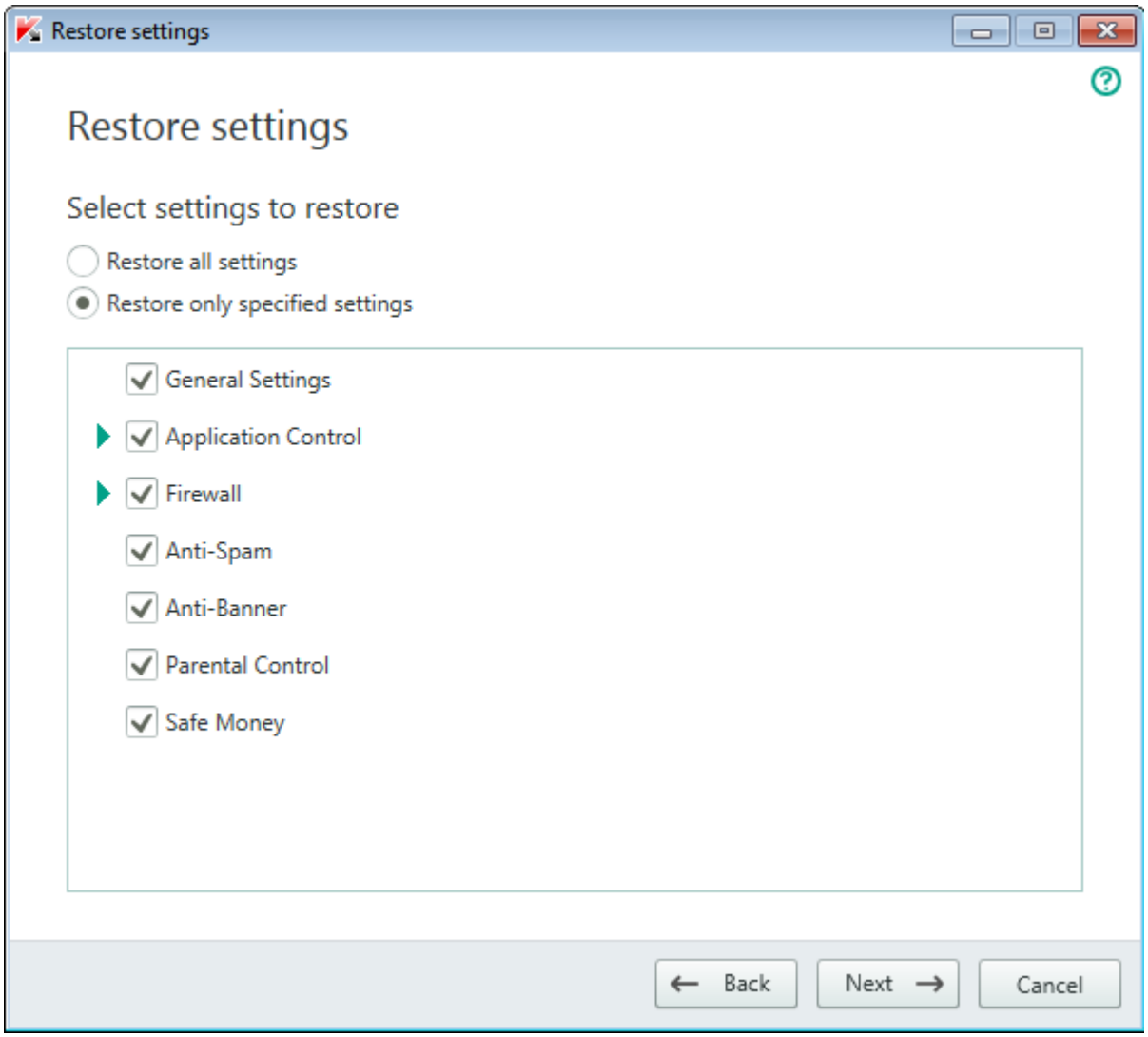
Oglejmo si korake čarovnika bolj podrobno.

1. korak. Zagon čarovnika

Kliknite gumb **Next** za zagon čarovnika.

2. korak. Ponovna vzpostavitev privzetih nastavitev

To okno čarovnika prikazuje, katere komponente zaščite Kaspersky Internet Security imajo nastavitve, ki se razlikujejo od privzetih vrednosti, zato ker jih je spremenil uporabnik ali aplikacija Kaspersky Internet Security na podlagi učenja (požarna pregrada ali zaščita pred neželeno pošto). Če so bile za katero od komponent ustvarjene posebne nastavitve, so tudi te prikazane v oknu (glej spodnjo sliko).



Slika 7. Okno za ponovno vzpostavitev privzetih nastavitev

Posebne nastavitve vključujejo sezname dovoljenih in prepovedanih besednih zvez ter naslovov, ki jih uporablja zaščita proti neželeni pošti, sezname zaupanja vrednih spletnih naslovov in telefonskih številk ponudnikov internetnih storitev, pravila za izjeme pri zaščiti, ki jih ustvarijo komponente aplikacije, ter pravila filtriranja, ki jih uporablja požarna pregrada za pakete in aplikacije.

Posebne nastavitve so ustvarjene pri delu z aplikacijo Kaspersky Internet Security v povezavi s posameznimi opravili in varnostnimi zahtevami. Podjetje Kaspersky Lab priporoča, da shranite svoje posebne nastavitve, ko znova vzpostavljate privzete nastavitve aplikacije.

Izberite potrditvena polja za nastavitve, ki jih želite shraniti, in kliknite gumb **Next**.

3. korak. Analiza operacijskega sistema

Ta korak zajema iskanje informacij o aplikacijah Microsoft Windows. Te aplikacije so dodane na seznam zaupanja vrednih aplikacij. Za aktivnosti, ki jih izvajajo zaupanja vredne aplikacije na operacijskem sistemu, ne veljajo nikakršne omejitve.

Po zaključeni analizi bo čarovnik samodejno odprl naslednji korak.

4. korak. Zaključena ponovna vzpostavitev

Po zaključenih opravilih lahko čarovnika zaprete tako, da kliknete gumb **Finish**.

OGLED POROČILA O DELOVANJU APLIKACIJE

Kaspersky Internet Security hrani poročila o delovanju za vsako komponento aplikacije. Z uporabo poročila lahko pridobite statistične podatke o delovanju aplikacije (na primer, koliko škodljivih elementov je bilo odkritih in nevtraliziranih v določenem časovnem obdobju, kolikokrat je bila aplikacija v enakem obdobju posodobljena, koliko neželenih sporočil je bilo odkritih in še mnogo več). Poročila se hranijo v šifriranem formatu.

Če si želite ogledati poročilo o delovanju aplikacije:

1. Odprite glavno okno aplikacije.
2. V spodnjem delu glavnega okna kliknite na povezavo **Show Additional Tools** za prikaz dodatnih orodij. Odpre se okno z orodji **(Tools)**.
3. V oknu **Tools** kliknite na povezavo **Report**, da se odpre okno **Reports**.

   V oknu **Reports** so prikazana poročila o delovanju aplikacije za tekoči dan (na levi strani okna) in za določeno časovno obdobje (na desni strani okna).
4. Če si želite ogledati podrobno poročilo o delovanju aplikacije, v zgornjem delu okna **Reports** kliknite na povezavo **Detailed reports**. Odpre se okno **Detailed Reports**.

V oknu **Detailed Reports** so prikazani podatki v obliki tabele. Za prilagojen ogled poročil lahko izbirate med različnimi možnostmi razvrščanja podatkov.

KAZALO

L

M

N

O

P

Q

R

S

T

U

V

W