

• • • • • **T** • • Com •

PC-cillin Internet Security 2005  
Vodič za korisnike

# Sadržaj

1.	Dobrodošli u svijet Trend Micro PC-cillin Internet Security 2005.....	3
1.1.	Uvod.....	3
1.1.1.	Kako sve PC-cillin Internet Security djeluje na vaše računalo? .....	4
1.1.2.	Što možete učiniti jednim klikom miša? .....	4
1.2.	Novosti u programu PC-cillin Internet Security .....	4
1.3.	Minimalni sistemski zahtjevi.....	5
1.4.	Osnovne radnje za početak korištenja programa .....	6
1.5.	Instalacija .....	6
1.6.	Registracija .....	7
1.7.	Ažuriranje komponenti.....	8
1.7.1.	Uključivanje i postavljanje proxy-postavki .....	9
1.8.	Nastavak korištenja programa PC-cillin.....	9
1.9.	Savjeti za sigurnije korištenje računala.....	10
2.	Upoznavanje s programskim funkcijama .....	11
2.1.	Kako Trend Micro PC-cillin Internet Security štiti vaše računalo?.....	11
2.2.	PC-cillin Internet Security: glavni prozor.....	12
2.3.	Korištenje Trend Micro PC-cillin Internet Securitya .....	12
2.4.	Upotreba PC-cillin ikone u Windows Trayu.....	13
2.4.1.	Ikone u Windows Trayu .....	14
2.5.	Pregled sistemskih informacija .....	14
2.5.1.	Informacije o verzijama komponenti .....	15
2.5.2.	Internet Security Status.....	15
2.5.3.	Antivirus Status .....	15
2.5.4.	Log-zapisi (Event Logs) .....	16
2.6.	Outbreak Warning System .....	17
2.7.	Online pomoć.....	17
2.8.	Služba za korisnike .....	18
3.	Zaštita datoteka i podataka .....	18
3.1.	Real-time Scan – neprekidna zaštita.....	18
3.2.	Mail Scan – zaštita elektroničke pošte .....	18
3.3.	Provjera cijelog računala.....	19
3.4.	Provjera mape (foldera) ili datoteke .....	19
3.5.	Unaprijed zadane radnje (Scan Tasks).....	20
3.6.	Detekcija spywarea i ostalih internetskih opasnosti .....	20
3.7.	Detekcija i uklanjanje trojanaca .....	21
3.8.	Provjera sigurnosnih propusta .....	21
3.9.	Zaštita vaših privatnih podataka .....	22
3.10.	Anti-spam .....	23
3.10.1.	Anti-spam za Outlook™ .....	24
4.	Zaštita internetske veze .....	25
4.1.	Osobni vatrozid (Personal Firewall).....	25
4.1.1.	Uključivanje osobnog vatrozida.....	25
4.1.2.	Osobni firewall-profil .....	26
4.2.	Zaustavljanje internetskog prometa .....	26
4.3.	Blokiranje mrežnih virusa.....	26
4.4.	Filtriranje neprikladnog web-sadržaja.....	27
4.4.1.	Blokiranje unaprijed zadanih web-kategorija .....	28
5.	Virusi .....	29
5.1.	Što učiniti kada se detektira virus na vašem računalu? .....	29
5.2.	Akcije s datotekama koje nije moguće očistiti .....	29
5.3.	Čišćenje boot-virusa.....	30
6.	Podrška .....	31

# Dobrodošli u svijet Trend Micro PC-cillin Internet Security 2005

## 1.1. Uvod

Trend Micro PC-cillin Internet Security štiti vaše računalo od internetskih prijetnji kao što su virus, spyware, hakerski napad i spam. Nadalje, PC-cillin Internet Security štiti vaše osobne podatke, blokira neželjene web-stranice, provjerava vama dostupne Microsoftove sigurnosne zakrpe te provjerava e-mail u potrazi za virusima. Ovaj program odlikuje spoj jednostavnog sučelja i snažne funkcionalnosti. Nove funkcije osiguravaju svaku internetsku i mrežnu vezu od virusa i neovlaštenih upada.

Neželjena reklamna e-pošta, takozvani spam, problem je koji smeta pri radu i povećava troškove. PC-cillin Internet Security sadržava jaku anti-spam kontrolu koja omogućuje filtriranje neželjene pošte.

PC-cillin Internet Security također je u stanju prepoznati i blokirati spyware, adware i ostale internetske prijetnje. Spyware je najčešće instaliran zajedno s programima preuzetim s interneta, a može pratiti informacije kao što su web-stranice kojima surfate ili kupnje koje obavljate preko interneta.

Private Data Protection omogućuje vam da odredite važne osobne informacije - poput broja kreditne kartice, kućne adrese ili telefonskog broja - koje ne želite poslati na internet putem weba ili u porukama. PC-cillin Internet Security blokirat će i pratiti sve pokušaje slanja takvih podataka.

Osim navedenoga, PC-cillin Internet Security uključuje provjeru odlazne (SMTP) pošte, koja štiti druge korisnike od mogućnosti zaraze putem e-mail poruke poslana s vašeg računala. Odnosno, PC-cillin Internet Security provjerava sve poruke i privitke prije nego što napuste vaše računalo.

PC-cillin Internet Security možete čak i daljinski kontrolirati na udaljenim računalima u svojoj privatnoj mreži te također prepoznati "uljeze", koristeći Home Network Control i Wi-Fi Detection funkcije.

Outbreak Warning System štiti vaše računalo od proboja najnovijih virusa i sigurnosnih prijetnji. Ova funkcija upozorava vas na mogućnost nove mrežne zaraze i podsjeća na ažuriranje programa kako biste spriječili zarazu.

Čak i prije nego što potpuno instalirate Trend Micro PC-cillin Internet Security, on provjerava vaš operativni sustav u potrazi za virusima i trojanskim programima. Kad je instaliran, PC-cillin Internet Security čuva vaše računalo od virusa pomoću niza unaprijed zadanih automatskih radnji.

### 1.1.1. Kako sve PC-cillin Internet Security djeluje na vaše računalo?

Prije nego što krenete s konfiguracijom, PC-cillin Internet Security učinit će sljedeće:

- potražiti viruse svaki put kada otvorite, kopirate, premjestite ili spremite datoteku
- zaštititi od skidanja zaraženih datoteka s interneta
- detektirati i očistiti trojanske programe
- blokirati spyware
- provjeriti vaše e-mail poruke dok se preuzimaju s POP3 servera (poslužitelja) ili šalju putem SMTP servera, te provjeriti privitke (attachment) preuzete preko nekog webmail servisa (provjerite odlomak "Minimalni sistemski zahtjevi" u nastavku kako biste vidjeli popis podržanih e-mail klijenata)
- zaštititi vaše računalo od napada s interneta koristeći osobni vatrozid (Personal Firewall)
- nadzirati Microsoft™ Word i Excel™ aplikacije u potrazi za makrovirusima koristeći MacroTrap™ tehnologiju koja detektira makroviruse putem heuristike (na temelju "ponašanja", umjesto uspoređivanja s uzorkom)
- provjeravati nepoznate viruse na temelju njihova ponašanja koristeći napredne heurističke metode
- pretraživati sve datoteke na vašem disku u skladu s predefiniranom radnjom pretrage (Scan Task)
- pretraživati sve programske datoteke u skladu s predefiniranom radnjom pretrage (Scan Task).

### 1.1.2. Što možete učiniti jednim klikom miša?

- provjeriti sve datoteke na svojem računalu
- provjeriti svaku datoteku iz Windows Explorera ili My Computera desnim klikom miša na ikonu datoteke
- provjeriti diskete (Floppy Disk)
- provjeriti sve Word ili Excel dokumente u potrazi za makrovirusima
- provjeriti svoje računalo u potrazi za spywareom, adwareom ili drugim internetskim prijetnjama.

## 1.2. Novosti u programu PC-cillin Internet Security

Kako virusi i ostali zlonamjerni programi postaju "pametniji", tako i Trend Micro PC-cillin Internet Security postaje napredniji kako bi omogućio potpunu zaštitu od virusa i internetsku sigurnost.

funkcija	opis
<b>Home Network Control</b>	Home Network Control omogućuje kontrolu podržanih Trend Micro proizvoda instaliranih na drugim računalima u vašoj mreži (LAN). Možete napraviti antivirusnu provjeru ostalih računala u mreži, ažurirati njihove komponente, kao i provjeriti imaju li Microsoftove sigurnosne propuste. Također, možete konfigurirati i pratiti Trend Micro postavke i log-zapise Trend Micro programa na ostalim umreženim računalima.

<b>Wi-Fi Detection</b>	Wi-Fi Detection prati vašu mrežu i upozorava vas na neželjene upade. Kako je pristup bežičnim mrežama mnogo lakši nego fizičkim, neželjeni upadi postali su ozbiljan sigurnosni problem. PC-cillin Internet Security provjeravat će vašu mrežu u intervalima koje vi odredite, i upozoriti vas ako se spoji novo računalo.
<b>Spyware Scan and Clean</b>	Mnoge internetske prijetnje nisu vezane samo uz viruse i sl. Naprotiv, tu su aplikacije koje ugrožavaju vašu privatnost, dopuštaju hakerima neovlašteni pristup računalu bez vašeg znanja, ili vas jednostavno ometaju u radu. Takvi programi najčešće su preuzeti s interneta i instalirani zajedno sa željenim programima, ali bez vašeg znanja. Ove prijetnje uključuju spyware, adware, dialere, joke-programe (šale), hakerske alate, programe za udaljeni pristup, aplikacije za probijanje lozinki itd. PC-cillin Internet Security omogućuje vam detekciju i čišćenje tih prijetnji, bilo ručno ili automatski preko Real-time Scana (automatska zaštita u pozadini).
<b>Lightweight Installation Mode</b>	<i>Lightweight Installation Mode</i> omogućuje instalaciju PC-cillin Internet Securitya samo s Real-time Scanom, za one koji žele samo antivirusnu i antispjware zaštitu, bez dodatnih mogućnosti.
<b>Security Vulnerability Check</b>	Ova funkcija pronalazi sigurnosne propuste koje je Trend Micro identificirao kao značajan rizik. Ti sigurnosni propusti ili "rupe" olakšavaju napadačima ili mrežnim virusima da nanesu štetu vašem računalu. Microsoft javno obznanjuje te slabe točke kao probleme koji postoje u njegovu softveru. Krpanje sigurnosnih rupa znatno smanjuje mogućnost napada ili zaraze virusima.
<b>Turbo Scan</b>	Turbo Scan vam dopušta ubrzanje ručne pretrage (Manual Scan) preskakanjem datoteka koje su već prije bile provjerene. Kada je Turbo Scan uključen, PC-cillin Internet Security vodi računa o datotekama koje su već bile provjerene. Ako nije bilo promjena na datoteci, neće biti ponovne provjere. To može značajno smanjiti vrijeme potrebno za izvršavanje jedne kompletne provjere (Manual Scan).

### 1.3. Minimalni sistemski zahtjevi

Sljedeći minimalni softverski i hardverski zahtjevi potrebni su za rad Trend Micro PC-cillin Internet Securitya:

#### operativni sistem

- Microsoft™ Windows™ XP Home ili Professional uz Service Pack 1 ili 2
- Windows 2000 Professional Service Pack 4
- Windows ME
- Windows 98SE
- Windows 98

#### procesor (CPU)

- Intel™ Pentium™ 233MHz ili ekvivalentni procesor pod Windows 98, 98SE, ME
- Intel Pentium 300MHz ili ekvivalentni procesor pod Windows 2000, XP

### **memorija**

- 64MB RAM (128 ili više preporučljivo) za Windows 98, 98SE, ME, 2000
- 128MB RAM za Windows XP

### **za sve instalacije**

- Internet Explorer 6.0 Service Pack 1 ili noviji
- 100 MB hard disk prostora za instalaciju
- podržani e-mail klijenti za Mail Scan, Anti-spam, i Private Data Protection - Microsoft Outlook™ Express 6.0, Microsoft Outlook 2002-2003, Netscape™ Mail 7.1, Eudora™ Pro 6.0, Becky!™ Internet Mail version 2
- Webmail Scan podržava sljedeće webmail servise - MSN Hotmail, Yahoo! Mail, AOL Mail
- Private Data Protection podržava programe za dopisivanje - Windows Messenger 4.7 i 5.0, MSN Messenger 6.2, ICQ Lite.

NAPOMENA: nužna je internetska veza radi registracije, ažuriranja i ostalih online servisa.

## **1.4. Osnovne radnje za početak korištenja programa**

U ovom je odlomku popis najvažnijih radnji koje valja poduzeti da biste osposobili Trend Micro PC-cillin Internet Security za rad. Kako biste učinkovito koristili ovaj program, Trend Micro preporučuje da napravite sve dolje navedene radnje kod prvog korištenja:

- instalacija – vidi u nastavku
- registracija softvera – daje pravo na ručno i automatsko ažuriranje komponenti
- ručno ažuriranje – redovito ažuriranje softvera osnovni je preduvjet učinkovite antivirusne zaštite
- ručna provjera računala – napravite pretragu cjelokupnog računala kako biste se uvjerali da nema virusa ili drugih zlonamjernih programa skrivenih na vašem računalu.

## **1.5. Instalacija**

Trend Micro PC-cillin Internet Security instalacija je jednostavna i traje samo nekoliko minuta.

**VAŽNO!** Prije instalacije uklonite sve postojeće antivirusne programe, uključujući i prijašnje verzije Trend Micro antivirusnog softvera, osim PC-cillin Internet Security 2004 ili PC-cillin Antivirus 2004 (koji će biti automatski uklonjeni).

Kako instalirati PC-cillin Internet Security?

1. a) Program na CD-u - umetnite PC-cillin Internet Security instalacijski CD u svoj CD-ROM uređaj i napravite sljedeće:
  - ako se instalacijski izbornik pojavi automatski, kliknite na Install Program, a zatim Next
  - ako se instalacija programa ne pokrene automatski, pokrenite ju iz Windows Taskbara klikom na Start > Run; potom u Open polju utipkajte D:\Setup\setup.exe i kliknite na OK (gdje je D vaš CD-ROM); zatim kliknite na Next.

b) Program na T-Com web-stranicama [www.t-com.hr](http://www.t-com.hr) - kad skinete program na svoje računalo, pronađite ga i dvaput kliknite na na ikonu aplikacije, što pokreće instalaciju.

2. Pročitajte licencni ugovor, a zatim kliknite na **I accept the terms in this licence agreement** (tj. "prihvaćam uvjete ovog licencnog ugovora") za nastavak instalacije. Instalacija će se prekinuti ako ne prihvatite uvjete ugovora.
3. Kliknite na **Next**. Prije instaliranja samog programa, PC-cillin Internet Security pregledava memoriju vašeg računala, boot-sektor i ključne datoteke. Ako ovdje PC-cillin Internet Security pronađe zaraženu datoteku, aktivirat će čišćenje, a potom, eventualno, i brisanje.
4. Pojavljuje se prozor **Registration Information** koji valja ispuniti na sljedeći način: u polje **User Name** unesite svoje ime, koje trebate obavezno upisati kako bi se nastavila instalacija
  - u polje **Organization** upišite ime svoje organizacije ili tvrtke
  - ako je u polje **Serial Number** upisan broj, taj broj nemojte brisati; kliknite na **Next**.
5. Pojavljuje se prozor **Installation Location**. Ovdje možete izabrati gdje će PC-cillin Internet Security biti instaliran, ili ostaviti unaprijed zadanu lokaciju. Za promjenu lokacije kliknite na **Change** i odaberite željenu lokaciju. Kliknite na **Next**.
6. Pojavljuje se **Installation Type** ekran. Ovdje možete instalirati punu verziju PC-cillin Internet Securitya, ili samo osnovnu antivirusnu funkciju. Ako odaberete **Antivirus Only**, neće biti instalirane funkcije kao što su Personal Firewall, Wi-Fi Detection i Emergency Center. Trend Micro preporučuje upotrebu te opcije samo ako koristite drugi postojeći firewall softver. Kliknite na **Next**.
7. Pojavljuje se **Configuration Type** ekran. Izaberite preporučenu konfiguraciju ili odaberite **Lightweight** mod koji aktivira samo funkcije Real-time Scan i Intelligent Update. Ove postavke možete u svakom slučaju promijeniti nakon instalacije. Kliknite na **Next**.
8. Ako ste zadovoljni s odabranim postavkama, odaberite **Install** za početak instalacije.
9. Nakon instalacije, čarobnjak vas informira da je instalacija uspjela, a PC-cillin Internet Security se pokreće. Kliknite na **Finish** za završetak instalacije.

Ako vas instalacija upita za restart računala, ugasi sve trenutačno otvorene programe te kliknite na **Yes** za restart.

## 1.6. Registracija

Odvojite nekoliko minuta za online registraciju, s kojom dobivate pravo na redovito ažuriranje svojeg programa.

**VAŽNO!** Registrirajte PC-cillin kako biste omogućili ažuriranje komponenti. Samo redovito ažuriranje osigurat će učinkovitu antivirusnu zaštitu.

## Kako registrirati Trend Micro PC-cillin Internet Security:

1. uvjerite se da ste ispravno spojeni na Internet
2. u glavnom prozoru PC-cillin Internet Security kliknite na **Updates and Registration > Registration**
3. provjerite je li vaš serijski broj ispravno upisan i kliknite na **Register Now**; ako ste se pretplatili na uslugu SURFAJTE SIGURNO, upišite serijski broj i kliknite na **Register Now**
4. u odgovarajuća polja na **Register** web-stranici upišite svoje ime, e-mail adresu i druge potrebne podatke
5. kliknite na **Preview** pa provjerite jesu li unesene informacije točne
6. kliknite na **Submit**
7. prikazuje se vaš serijski broj, a potvrda se šalje ne prethodno upisanu e-mail adresu.

Registrirali ste se i postali član Trend Micro Customer Care Centera. Sada možete redovito ažurirati PC-cillin Internet Security.

## 1.7. Ažuriranje komponenti

Kako biste zaštitili svoje računalo od najnovijih prijetnji, pravodobno ažurirajte komponente: program files, scan engine, virus pattern file (tj. datoteku s definicijama virusa), kao i ostale komponente potrebne za učinkovitu zaštitu.

Trend Micro izdaje novi pattern file najmanje jednom tjedno. Ažuriranje pattern filea omogućuje detekciju najnovijih virusa i ostalih zlonamjernih programa.

**VAŽNO!** Kako Trend Micro svaki mjesec otkriva stotine novih virusa, neophodno je redovito ažurirati PC-cillin Internet Security komponente.

### Ručno ažuriranje virusnog pattern filea (datoteke uzoraka) i scan enginea:

1. u glavnom prozoru PC-cillin Internet Security kliknite na **Update Components** i pojavit će se **Update** prozor; ako proces ažuriranja nije započeo, kliknite na **Update** - na prozoru se vidi tijek ažuriranja
2. za zaustavljanje ažuriranja kliknite na **Stop**, a kako biste iznova nastavili s ažuriranjem, kliknite na **Update**.

PC-cillin omogućuje i automatsko ažuriranje u unaprijed zadanim intervalima pomoću funkcije **Intelligent Update**. Ova moćna funkcija održava PC-cillin Internet Security i sve njegove komponente ažurnima i time pruža maksimalnu zaštitu uz minimalnu intervenciju korisnika.

### Podešavanje redovitog ažuriranja:

1. u glavnom prozoru PC-cillin Internet Security kliknite na **Updates and Registration > Update Settings**
2. odaberite **Enable Intelligent Update** i odredite koliko će često PC-cillin Internet Security provjeravati dostupnost novih komponenti za ažuriranje
3. kliknite na **Apply**.

## 1.7.1. Uključivanje i postavljanje proxy-postavki

Proxy-server koristi se radi dodatne razine sigurnosti i poboljšanja performansi mreže. Većina kućnih korisnika nema proxy-server, međutim, on nije rijetkost u većim organizacijama, tj. u poslovnom okruženju. Stoga, ako imate problema sa spajanjem na internet radi ažuriranja komponenti ili registracije proizvoda, možda imate proxy-server koji nije identificiran ili je došlo do greške prilikom autentifikacije na tom proxyju.

Ako koristite proxy-server, zapišite IP adresu i priključnicu (engl. port) servera, te korisničko ime i lozinku - ukoliko proxy traži autentifikaciju.

### Za uključivanje i postavljanje proxy-postavki napravite sljedeće:

1. u PC-cillin Internet Security glavnom prozoru kliknite na **Updates and Registration > Update Settings**
2. pod Proxy Information odaberite **Use a Proxy Server...**
3. kliknite na **Proxy Settings** i napravite sljedeće:
  - u polje **Proxy Address** unesite IP adresu servera ili puno ime (npr. proxy.mydomain.com)
  - u polje **Port** upišite broj porta (primjerice 8080)
  - u poljima **User name** i **Password** upišite korisničko ime i lozinku, ako je potrebno
4. kliknite na **OK**
5. kliknite na **Apply**.

**NAPOMENA:** Za konfiguraciju proxy-servera u kontekstu Personal Firewall funkcije procedura je slična gornjoj. Za detaljne upute pogledajte online pomoć pod Guarding Against Internet Attacks > Managing Personal Firewall Profiles > Configuring a Proxy Server.

## 1.8. Nastavak korištenja programa PC-cillin

Nakon što ste se uvjerali u sigurnost programa, pretplatite se na uslugu SURFAJTE SIGURNO. Kliknite na **Buy Now** u prozoru koji se pojavljuje prilikom pokretanja PC-cillin Internet Securitya 2005, te slijedite upute na zaslonu.

### Online

Ako ste postojeći MAXadsl ili dial-up korisnik, na korisničkim stranicama <http://www.t.com.hr/user> možete se jednostavno online pretplatiti na uslugu SURFAJTE SIGURNO, bez dodatnih potpisa.

Identificirate se svojim korisničkim imenom i lozinkom te ispunite svoje podatke (ime, e-mail, adresa, kontakt), odaberete način plaćanja usluge, potvrdite dodatne uvjete i pretplatite se na uslugu. Na navedenu e-mail adresu stiže vam serijski broj koji unesete u program na način opisan u poglavlju 1.6. Registracija. Serijski broj za uslugu uključuje pravo na ažuriranje (updates), pattern fileove i osnovnu tehničku podršku.

## Osobno

Novi i postojeći MAXadsl te dial-up korisnici mogu jednostavno podnijeti zahtjev i potpisati ugovor za uslugu SURFAJTE SIGURNO u T-Centrima i T-Partnerima.

U T-Centrima serijski broj dobiju odmah. Kod T-Partnera ispune zahtjev i potpišu ugovor, a serijski broj dobiju putem e-maila koji su naveli u zahtjevu.

## 1.9. Savjeti za sigurnije korištenje računala

- **Real-time Scan mora biti uključen** – Real-time Scan pruža neprekidnu zaštitu od virusa u pozadini. S uključenim Real-time Scanom značajno se smanjuje mogućnost zaraze računala. Zbog njegovih velikih mogućnosti (i zato što radi neprimjetno, u pozadini), Trend Micro preporučuje da Real-time Scan uvijek bude uključen.
- **Ažurirajte Trend Micro PC-cillin Internet Security** – Registrirajte PC-cillin i skidajte najnovije verzije pattern filea, scan enginea i komponenti programa, koji osiguravaju da PC-cillin koristi najnoviju tehnologiju zaštite. Uz to, podesite PC-cillin tako da automatski skida dopune koristeći Intelligent Update.
- **Čuvajte se sumnjivih e-mail privitaka (attachmenta)** – E-mail je najčešći način širenja virusa i zlonamjernih programa. Ako dobijete e-mail poruku od nekoga koga ne poznajete, ne smijete pokretati ili spremati datoteke u attachmentu. Osim toga, bez obzira na to tko vam je poslao e-mail, pripazite na attachmente koji sadrže izvršne datoteke (exe, com, pif, scr).
- **Podesite vrijeme zakazane provjere programa (Scheduled Scan)** – Scan Tasks funkcija je brz i jednostavan način da se uredi veliki broj planiranih provjera (Scan Tasks) vašeg računala. Koristeći Scan Tasks, moguće je definirati vrstu datoteka koje se provjeravaju te koliko često. Primjerice, možete podesiti da se pretražuju sve datoteke na računalu svakog petka u deset sati navečer.
- **Budite obaviješteni** – Redovito posjećujte Trend Micro internetske stranice ([www.trendmicro.com](http://www.trendmicro.com)) kako biste dobili informacije o najnovijim virusima i sigurnosnim događajima. Uz to, na ovim stranicama nalazi se i Trend Micro Virusna enciklopedija.
- **Ažurirajte Windowse** – Microsoft reagira na sigurnosne probleme unutar svojeg softvera tako što redovito izdaje sigurnosne zakrpe za najnovije sigurnosne propuste. Microsoft Windows operativni sustav omogućuje Windows Update funkciju koja vam dopušta da automatski ažurirate sustav. Koristite PC-cillin funkciju Security Check kao biste utvrdili je li vaše računalo ažurirano.

## 2. Upoznavanje s programskim funkcijama

### 2.1. Kako Trend Micro PC-cillin Internet Security štiti vaše računalo?

PC-cillin Internet Security štiti vaše računalo od vanjskih i unutarnjih prijetnji

prijetnja	PC-cillin Internet Security zaštita
vanjska (dolazna) – virusi i drugi zloćudni programi kao što su trojanci i crvi te zaraženi e-mail ili attachment	Real-time Scan provjerava svaku datoteku koja je downloadirana, kopirana ili premještena na vaš kompjuter.  Mail Scan provjerava dolazni (POP3) i odlazni (SMTP) mail za viruse. Webmail Scan osigurava zaštitu od zaraženih webmail attachmenta (privitaka).
unutarnji (lokalni) virusi i zlonamjerni programi (npr. trojanci [Trojan horse], crvi [worms])	Ručna provjera (Manual Scan) i predefiniрана provjera (Scheduled Task) kontroliraju vaše računalo lokalno.  PC-cillin Internet Security za trojance popravlja štete unutar operativnog sustava nastale djelovanjem trojanaca, zaustavlja njihove procese te briše datoteke koje je trojanac instalirao.
virusne epidemije	Outbreak Warning System je funkcija koja vas preventivno upozorava na virusne epidemije ili druge visokorizične situacije te vas savjetuje da što hitnije ažurirate svoj PC-cillin.  Možete i trenutačno zaustaviti sav internetski promet, ako sumnjate na epidemiju ili neku drugu sumnjivu aktivnost.
hakerski upadi u računalo	Osobni firewall (vatrozid) osigurava zaštitu od vanjskih napada. Popis iznimaka omogućuje vam da konfigurirate svoj vatrozid prema vlastitim potrebama.
neprikladne internetske stranice	URL Filter omogućuje vam da blokirate pristup neprikladnim internetskim stranicama. Možete napraviti popis zabranjenih i dopuštenih stranica ili pak koristiti već definirane kategorije.
spam e-mail poruke	PC-cillin Internet Security Anti-spam Engine prepoznaje spam e-maile i označava ih kao takve.
prikupljanje osobnih podataka	Funkcija Private Data Protection omogućuje vam da definirate svoje osobne podatke (kao što su broj kreditne kartice ili kućna adresa) čije će slanje preko interneta PC-cillin blokirati.
Wireless Ethernet (Wi-Fi) upadi u mrežu	Wi-Fi detekcija provjerava vašu mrežu kako bi utvrdila tko je spojen na nju. Firewall profili daju vam

	fleksibilnost u promjeni postavki vašeg osobnog firewalla, ovisno o radnom okruženju. Primjerice, možete konfigurirati Wi-Fi profil koji će vam pomoći u zaštiti vašeg računala prilikom pristupa neprovjerenom LAN-u.
poznati Microsoftovi sigurnosni propusti	Security Check provjerava ima li vaše računalo sigurnosne propuste koji omogućuju virusima ili hakerima neovlašteni pristup. Microsoft javno objavljuje ove sigurnosne propuste u svojem softveru.
spyware i ostale internetske prijetnje	PC-cillin Internet Security otkriva i uklanja spyware, adware i ostale prijetnje s interneta koje se instaliraju prilikom downloada legitimnih internetskih programa. Spyware prati vaše osobne podatke, kao što su internetske stranice koje posjećujete ili što kupujete preko interneta. Ostale opasnosti iz te kategorije omogućuju hakerima da preuzmu udaljenu kontrolu nad vašim računalom bez vašeg znanja ili da vam jednostavno smetaju pri radu.


## 2.2. PC-cillin Internet Security: glavni prozor

Sučelje PC-cillin Internet Securitya omogućuje brz pristup svim antivirusnim i sigurnosnim postavkama.

### Za pristup glavnom prozoru PC-cillin Internet Security:

- na Windows traci s alatima kliknite na **Start > Programs > Trend Micro > PC-cillin > Trend Micro PC-cillin Internet Security 2005**

ili

Na sistemskoj traci /  (System Tray) desnom tipkom svojeg miša kliknite na ikonu PC-cillin Internet Security te kliknite na **Open Main**. (Sistemska traka nalazi se pokraj sata u donjem desnom kutu vašeg zaslona.)







## 2.3. Korištenje Trend Micro PC-cillin Internet Securitya

Novo korisničko sučelje pruža brz pristup svim postavkama i informacijama. Na vrhu glavnog prozora nalaze se poveznice (linkovi) za funkcije koje se najčešće koriste:

link (poveznica)	opis
<b>Scan for Viruses</b>	Pretražuje vaše računalo prema prethodno definiranim postavkama za ručno pretraživanje (Manual Scan Settings).
<b>Update Components</b>	Provjerava najnoviji Virus Pattern File (najnoviju datoteku virusnih uzoraka) i ostale komponente na Trend Micro Active Update serveru, internetskom serveru gdje su locirane dopune (updates) Trend Micro

	proizvoda. Potreban je pristup internetu.
<b>Scan for Spyware</b>	Pretražuje vaše računalo tražeći spyware, adware i druge internetske prijetnje.
<b>Help</b>	Osigurava brz pristup online pomoći (Online Help), informacijama o proizvodu te drugim online resursima.

Svaka od funkcijskih tipki na lijevoj strani glavnog prozora omogućuje vam upravljanje funkcijom za određeno sigurnosno područje.

za izvršavanje sljedećih radnji...	...kliknite na
pogledajte status svojih antivirusnih i sigurnosnih postavki, kao i log-zapise	 <b>Summary</b>
konfigurirajte Scan Settings i karantenu, Scan Tasks, traži Spyware i sigurnosne propuste	 <b>System</b>
konfigurirajte Mail Scan, Web Scan i Anti-spam Scan	 <b>Email</b>
konfigurirajte URL filter, zaštitu osobnih podataka, kontrolu kućne mreže (Home Network Control) i definiranje zaporki (Passwords).	 <b>Network Control</b>
konfigurirajte osobni firewall i Wi-Fi detekciju; postavke Emergency Center funkcije	 <b>Network Security</b>
postavke za ažuriranje, izvršite Manual Scan i registrirajte svoj softver	 <b>Updates and Registration</b>




## 2.4. Upotreba PC-cillin ikone u Windows Trayu

Najbrži način pristupa nekim funkcijama PC-cillin Internet Securitya je preko ikone u tzv. Windows Trayu (u pravilu donji desni dio ekrana). Npr. moguće je otvoriti glavni prozor, ili dobiti informaciju je li uključen Real-time Scan.

<b>kako biste:</b>	<b>napravite sljedeće:</b>
otvorili glavni prozor	desni klik na Task Tray ikonu i kliknite na <b>Open Main</b>
izašli iz PC-cillin Internet Securitya	desni klik na Task Tray ikonu i kliknite na <b>Exit</b>
zaustavili internetski promet	desni klik na Task Tray ikonu i kliknite na <b>Halt Internet Traffic</b>
obavili ažuriranje	desni klik na Task Tray ikonu i kliknite na <b>Update Component</b>
pretražili računalo za virusima	desni klik na Task Tray ikonu i kliknite na <b>Scan for Viruses</b>
provjerili računalo za Microsoftove sigurnosne propuste	desni klik na Task Tray ikonu i kliknite na <b>Check Security</b>
promijenili profil osobnog firewalla	desni klik na Task Tray ikonu i kliknite na <b>User Profile, te odaberite novi profil</b>
uključili ili isključili Real-time Scan	desni klik na TaskTray ikonu i kliknite na <b>Real-time Scan</b>

## 2.4.1. Ikone u Windows Trayu

U sljedećoj tablici opisana su značenja pojedinih ikona u Windows Trayu.

<b>ikona</b>	<b>opis</b>
	sav dolazni i odlazni internetski promet je zaustavljen
	spajanje na Trend Micro server kako bi se program ažurirao
	Real-time Scan je uključen
	Real-time Scan je isključen (siva munja)

## 2.5. Pregled sistemskih informacija

PC-cillin Internet Security nudi vam sažete i detaljne informacije o statusu antivirusa i internetske sigurnosti. Možete pregledati sažete informacije kako biste vidjeli koje su postavke uključene ili pak možete pogledati log-zapise za detaljne informacije o događajima.

## 2.5.1. Informacije o verzijama komponenti

Budite sigurni da su Pattern File, Scan Engine i ostale komponente ažurne.

### Pregled informacija o verzijama:

- **kliknite na Help > About**

Uz informacije o verzijama, ovdje možete vidjeti svoj serijski broj, koji vam je potreban prilikom kontaktiranja tehničke podrške ili ako želite reinstalirati svoj PC-cillin Internet Security.

Kako biste vidjeli koji je najnoviji Pattern File ili Scan Engine dostupan, posjetite Trend Micro Virus Information Center:

- kliknite na **Help > Virus Information Center**.

## 2.5.2. Internet Security Status

Prozor Internet Security Status prikazuje kratak pregled statusa internetskih sigurnosti. Omogućuje brzu provjeru sigurnosti vašeg računala u sljedećim područjima: Personal Firewall (osobni vatrozid), URL Filter, Private Data Protection, Wi-Fi Detection i Anti-spam.

### Pregled prozora Internet Security Status

- kliknite na **Summary > Internet Security Status**.

Okvir **Last Attack Information** prikazuje najnoviji pokušaj napada ili udaljenog ispitivanja vašeg računala (scan). Ova se informacija prikazuje samo ako je uključen Personal Firewall.

Okvir Internet **Security Settings** prikazuje trenutni status Internet Security postavki (enabled/disabled). Možete kliknuti na svaki od linkova koji vodi do konfiguracijskog prozora za svaku postavku.

Okvir Internet **Traffic Monitoring** prikazuje ukupnu količinu poslanog i primljenog prometa. Povećani promet, dok se ne koristi internet, može upućivati na aktivnost virusa.

## 2.5.3. Antivirus Status

Prozor Antivirus Status prikazuje sažetak antivirusnih postavki i postavki ažuriranja. Koristite ovaj prozor za opću provjeru statusa antivirusnih postavki, kao i za uvid u antivirusne statistike.

## Pregled prozora Antivirus Status

- kliknite na **Summary > Antivirus Status**.

Okvir **Scan and Virus Status** prikazuje informacije o zadnjem pronađenom virusu i zaraženoj datoteci, zatim o posljednjoj provjerenoj datoteci, kao i vrijeme posljednje ručne ili zakazane provjere.

Okvir **Update and Scan Settings** prikazuje trenutno stanje antivirusnih postavki (uključeno/isključeno). Kliknite na link koji vodi do konfiguracijskog prozora za svaku pojedinu postavku.

## 2.5.4. Log-zapisi (Event Logs)

Trend Micro PC-cillin Internet Security čuva log-zapise za sljedeće događaje: ažuriranje (Update), Antivirus, URL Filter, Trojan Cleanup Service, Private Data Filter, Anti-spam i Personal Firewall. Ovi se zapisi mogu pregledavati preko prozora Event Logs i čine važan izvor informacija. Naprimjer, moguće je saznati je li pronađen virus trojanac ili crv, te je li izbrisan ili prebačen u karantenu.

### Pregled log-zapisa:

1. u glavnom prozoru kliknite na **Summary > Event Logs**
2. odaberite vrstu log-zapisa iz padajuće liste
3. kliknite na **View Logs**
4. odaberite datum zapisa.

Osim što daje informaciju o vremenu svakog zapisa, svaka vrsta zapisa nudi sebi svojstvene informacije:

log-zapis	Bilježi se kada...
<b>Virus</b>	...je detektiran virus ili drugi zlonamjerman program. Virus log-zapisi također sadrže vrijeme kada je virus detektiran, vrstu provjere (Real-time ili Manual) koja je pronašla virus, vrstu virusa, ime virusa, ime datoteke u kojoj je pronađen virus, status prve akcije i, eventualno, druge akcije.
<b>Update (ažuriranje)</b>	...pokušate ažurirati proizvod najnovijim komponentama. Log-zapis također sadrži informacije o datotekama koje su ažurirane i instalirane, kao i rezultat ažuriranja (uspješno/neuspješno).
<b>Personal Firewall</b>	...je računalo napadnuto s interneta. Personal Firewall log-zapisi sadrže vrstu vatrozidne obrane, vrijeme napada, vrstu korištenog protokola, izvornu ip adresu i port, odredišnu ip adresu i port, razlog blokiranja prometa, kao i putanju te ime napadnute aplikacije.
<b>Anti-spam</b>	...je detektiran spam i označen kao takav. Anti-spam log-zapisi sadrže vrijeme detekcije, subject-polje poruke i pošiljatelja.
<b>URL filter</b>	...Web site je blokiran ili je detektiran zlonamjerni program u web-prometu. URL filter-zapisi sadrže vrijeme detekcije, korištenu filter-postavku, blokirani URL, kao i pripadajuću kategoriju za

	URL.
<b>Trojan Cleanup</b>	...Trojan Cleanup Service/Damage Cleanup Service (DCS) je detektirao trojanca. DCS detektira i automatski čisti trojanca. DCS log-zapisi sadrže vrijeme detekcije, ime trojanca te rezultat čišćenja.
<b>Private Data Protection</b>	...računalo pokušava poslati privatne podatke preko interneta. Ovi log-zapisi sadrže vrijeme pokušaja slanja, vrstu podataka, kao i web site ili mail adresu na koju su podaci pokušani poslati.
<b>Spyware</b>	...kada je detektiran spyware ili druga internetska opasnost. Ovi zapisi sadrže vrijeme detekcije, ime opasnosti i rezultat čišćenja.
<b>Security Check</b>	...kada je detektiran Microsoftov sigurnosni propust. Ovaj zapis sadrži vrijeme detekcije, ime Microsoftova bulletina (tj. upozorenja) povezanog s ovim propustom, procjenu rizika te imena zlonamjernih programa koji iskorištavaju taj propust.

**NAPOMENA:** log-zapise možete razvrstati (rastući ili padajući kriterij) po stupcu (npr. vrijeme zapisa), i to tako što kliknete na naslov pojedinog stupca.

## 2.6. Outbreak Warning System

Trend Micro PC-cillin Internet Security uključuje inovativnu uslugu prevencije najnovijih virusnih epidemija te drugih zlonamjernih programa. Koristeći istraživanja i znanje tvrtke TrendLabs, PC-cillin Internet Security može proaktivno upozoriti na najnoviju opasnost kako biste stigli na vrijeme ažurirati proizvod i tako spriječiti infekciju.

Omogućite Outbreak Warning kako biste dobivali upozorenja o virusnoj epidemiji (Outbreak Warning):

1. u glavnom prozoru PC-cillin Internet Security kliknite na **Updates and Registration > Outbreak Warning Settings**
2. odaberite **Enable Outbreak Alert**
3. kliknite na **View Alert**, kako biste pregledali najnovije upozorenje o epidemiji
4. kliknite na **Apply**.

Upozorenja o epidemiji klasificirana su kao "crveno" ili "žuto" upozorenje (Red Alert, Yellow Alert). Crveno upozorenje znači visok, a žuto srednje visok rizik.

**VAŽNO!** Ako dobijete upozorenje o epidemiji, odmah ažurirajte PC-cillin, a zatim napravite antivirusnu provjeru računala.

## 2.7. Online pomoć

Online pomoć u sklopu Trend Micro PC-cillin Internet Security pokriva sve funkcije i karakteristike programa. Online pomoć možete koristiti za pitanja koja imate u vezi s programom.

**Pristup online pomoći:**

- na glavnom prozoru PC-cillin Internet Security kliknite na **Help > Contents and Index**.

Koristeći program, na pojedinim mjestima naići ćete na gumbе za pomoć. Kliknite na njih kako biste došli do informacija o trenutаčno otvorenom prozoru.



## 2.8. Služba za korisnike

Ako imate pitanja ili želite dodatne informacije o korištenju usluge SURFAJTE SIGURNO, tj. o programu PC-cillin, nazovite Službu za korisnike na besplatni telefon 0800 9000, fax 0800 9009 ili e-mail kontakt@t-com.hr

## 3. Zaštita datoteka i podataka

### 3.1. Real-time Scan – neprekidna zaštita

Real-time Scan je neprekidna zaštita računala od virusa koja pregledava sve datoteke što se kopiraju, skidaju s interneta (download) ili prebacuju na vaše računalo. Real-time zaštita sve vrijeme radi u pozadini, bez ikakve intervencije korisnika. To znači da ne trebate ništa poduzeti kako biste koristili Real-time zaštitu, osim provjeriti je li uključena.

Kako biste provjerali status real-time zaštite, pogledajte PC-cillin ikonu u Windows trayu (u nastavku desni dio ekrana):



**Real-time zaštita je aktivirana (enabled)**  
crvena munja



**Real-time zaštita je isključena (disabled)**  
siva munja

#### Kako aktivirati Real-time zaštitu:

- u Windows sistem trayu (dolje desno) desnom tipkom miša kliknite na PC-cillin ikonu i zatim odaberite Real-time Scan.

### 3.2. Mail Scan – zaštita elektroničke pošte

E-mail je najčešći izvor zaraze virusima i drugim zlonamjernim programima, poglavito ako otvarate e-mail poruke ili prilitke (attachment). Zbog popularnosti e-mail komunikacije, pisci virusa stvaraju viruse koji iskorištavaju poznate sigurnosne propuste unutar e-mail programa.

Mail Scan funkcija služi za provjeru e-mail poruka i attachmenta dok se primaju ili šalju preko POP3/SMTP mail servera. Podržani e-mail programi su:

- Microsoft Outlook 2000 ili noviji
- Outlook Express 6.0 Service Pack 1 ili noviji

- Eudora Pro 6.1 ili noviji
- Netscape Mail 7.1 ili noviji

Mail Scan također pretražuje privitke skinute s nekog web mail servisa (tj. mail spremljen na serveru kojemu se pristupa preko web-preglednika). Podržani web mail servisi su:

- MSN Hotmail
- Yahoo! Mail
- AOL Mail

Provjerite je li Mail Scan funkcija aktivirana:

- u glavnom prozoru kliknite na **E-mail > Mail Scan**
- kliknite na **Incoming Mail** - mora biti odabran **Enable Incoming Mail Scanning**
- kliknite na **Outgoing Mail** - mora biti odabran **Enable Outgoing Mail Scanning**
- kliknite na **Apply**.

### 3.3. Provjera cijelog računala

Možete napraviti provjeru svih diskova na računalu kako biste bili sigurni da nije zaraženo. Jednim klikom, PC-cillin omogućuje brzu i jednostavnu antivirusnu provjeru svih diskova spojenih na računalo:

- u glavnom prozoru kliknite na **Scan for Viruses**. PC-cillin će početi provjeru računala, a na ekranu će se pojaviti okvir Scan Files. Provjeru možete prekinuti u svakom trenutku, klikom na Stop.

**NAPOMENA:** PC-cillin Internet Security provjerava računalo na temelju Manual Scan postavki. Upute za promjenu tih postavki nalaze se u online pomoći pod knjigom "Protecting Against Viruses and other Threats > Configuring Scan Settings".

### 3.4. Provjera mape (foldera) ili datoteke

Možete napraviti i provjeru određene mape (uključujući i podmape/subfoldere) ili pojedine datoteke. PC-cillin Internet Security provjerava mape ili datoteke na temelju Manual Scan postavki.

**Za provjeru mape:**

- kliknite na desnom tipkom miša na određenu mapu i zatim odaberite **Scan for Viruses**.

**SAVJET:** isti učinak možete dobiti odvučete li folder na glavni prozor PC-cillina.

**Za provjeru pojedine datoteke:**

- kliknite na desnom tipkom miša na datoteku i zatim odaberite **Scan for Viruses**.

**SAVJET:** isti učinak možete dobiti kliknete li desnom tipkom miša na datoteku, odaberete Properties, a potom tab Virus Property; također možete i odvući datoteku na glavni prozor PC-cillina.

## 3.5. Unaprijed zadane radnje (Scan Tasks)

Ova funkcija omogućuje definiranje različitih vrsta provjere koje se automatski obavljaju u određeno vrijeme. Uz to, u svako vrijeme možete ručno "odvrtjeti" prethodno definirani zadatak ili radnju.

PC-cillin Internet Security nudi nekoliko unaprijed zadanih zadataka provjere. Osim što ih možete ručno pokrenuti, uvid u njihovu konfiguraciju dat će vam ideju kako učinkovito kreirati vlastite zadatke, odnosno radnje.

### Kako pokrenuti unaprijed zadanu radnju:

- u glavnom prozoru kliknite na **System > Manual Scan**
- s padajuće liste odaberite radnju koju želite obaviti
- kliknite na **Scan**. Provjeru zaustavljate klikom na **Stop**.

**NAPOMENA:** više o unaprijed zadanim radnjama (Scan Tasks) pronaći ćete u online pomoći pod knjigom "Protecting Against Viruses and other Threats > Managing Scan Tasks".

## 3.6. Detekcija spywarea i ostalih internetskih opasnosti

Mnoge internetske opasnosti nisu samo virusi i ostali srodni zlonamjerni programi. Naprotiv, često su to aplikacije koje ugrožavaju privatnost, dopuštaju hakerima neovlašteni pristup računalu bez vašeg znanja, ili jednostavno stvaraju smetnje pri radu. Pokatkad se neopaženo skidaju s interneta zajedno sa željenim programima (dolaze u paketu). Te opasnosti uključuju spyware, adware, dialere, joke-programe (šale), hakerske alate, alate za udaljeni pristup, aplikacije za probijanje passworda (zaporki) itd.

Trend Micro PC-cillin Internet Security detektira te opasnosti u sklopu Real-time Scan aktivnosti, a po potrebi može obaviti ručnu provjeru (Manual Scan) posebno za spyware i dodatne internetske opasnosti.

### Kako omogućiti Real-time provjeru spywarea i ostalih internetskih opasnosti:

- u glavnom prozoru PC-cillina kliknite na **System > Scan Settings**
- odaberite tab **Real-time Scan**
- kvačica na **Enable Real-time Scan** mora biti označena
- kliknite na tab **Spyware**
- odaberite **Enable for Spyware and Additional Internet Threats**
- označite kategorije opasnosti za koje želite provjeru
- kliknite na **Apply**.

### Ručna provjera spywarea i ostalih internetskih opasnosti:

- u glavnom prozoru PC-cillina kliknite na **Scan for Spyware**
- pojavit će se okvir **Spyware Scan Results** s ispisom svih pronađenih opasnosti
- za više informacija o pronađenoj opasnosti odaberite **More Information**
- odaberite opasnosti koje želite ukloniti

- kliknite na **Remove**.

**NAPOMENA:** sve pronađene aplikacije ne moraju biti uistinu štetne. Prije nego što ih uklonite, provjerite jesu li stvarno nepoželjne.

## 3.7. Detekcija i uklanjanje trojanaca

Trend Micro PC-cillin Internet Security detektira trojansku aktivnost, vraća datoteke koje su trojanci modificirali, zaustavlja trojanske procese te briše zaostale datoteke.

Trojanci, ili trojanski konji, mali su, naizgled bezopasni programi. Kako bi prouzročili ikakvu štetu, ti programi trebaju biti instalirani na vaše računalo. Jednom kada je trojanac instaliran, ima iste ovlasti kao i korisnik računala te može učiniti nešto što korisnik nije namjeravao. Glavna razlika između trojanca i virusa jest ta da se trojanci ne mogu replicirati i širiti samostalno.

PC-cillin Internet Security detektira trojance prilikom početne instalacije, a možete PC-cillin konfigurirati tako da ih automatski detektira prilikom ručnog pretraživanja, kao i svaki put kada se pokrene Real-time Scan.

### Za automatsku detekciju i brisanje trojanaca prilikom skeniranja:

- u glavnom prozoru PC-cillin Internet Security kliknite na **System > Scan > Settings**
- kliknite na **Manual scan** ili **Real-time Scan**, ovisno o tome na kojoj vrsti provjere želite uključiti detekciju trojanaca. Trend Micro preporučuje da uključite detekciju trojanaca za ručnu i Real-time provjeru.
- označite **Search for and Clean Trojans**
- kliknite na **Apply**.

### Ručno pretraživanje i brisanje trojanaca:

- locirajte mapu u kojoj je instaliran PC-cillin Internet Security (npr. Default mapa je C:\Program Files\Trend Micro\Internet Security 2005)
- dvostruki klik na datoteku **tsc.exe**
- konzolni prozor prikazuje tijek provjere.

## 3.8. Provjera sigurnosnih propusta

Sigurnosni propusti ili sigurnosne rupe olakšavaju napadačima, virusima i ostalim prijetnjama s interneta da naštetite vašem računalu. Microsoft redovito javno obznanjuje sigurnosne propuste, kao greške koje postoje u njihovu softveru. Krpanje sigurnosnih rupa uvelike smanjuje mogućnost zaraze ili napada.

PC-cillin Internet Security provjerava vaše računalo na sigurnosne propuste za koje Trend Micro smatra da predstavljaju značajan rizik. Kada pronađe sigurnosni propust, PC-cillin prikazuje razinu rizika, potencijalnu opasnost te broj Microsoftovih izvještaja o propustu (tzv. bulletin).

**Risk Level** (razina rizika) predstavlja razine rizika za pojedini sigurnosni propust. Te razine su u padajućem popisu poredane po razini opasnosti:

- **Critical**
- **Very high**
- **High**
- **Moderate**
- **Low**

**Potential Threat (potencijalna opasnost)** prikazuje poznate viruse ili druge prijetnje koje iskorištavaju navedeni sigurnosni propust. Za više informacija o potencijalnoj prijetnji konzultirajte Trend Micro Virusnu enciklopediju.

**Related Bulletin (Microsoftov izvještaj)** daje referentni broj (Reference Number) Microsoftova Security Bulletina koji opisuje taj sigurnosni propust. Za pregled izvještaja posjetite Microsoftove web-stranice.

**Provjerite svoje računalo na Microsoftove sigurnosne propuste:**

- u glavnom prozoru PC-cillin Internet Security kliknite na **System > Security Check**
- kliknite na **Check**
- rezultat pogledajte u **Security Check Results**

### 3.9. Zaštita vaših privatnih podataka

Private Data Protection funkcija omogućuje vam definiranje određenih vrsta informacija (npr. vaše ime, adresa ili broj kreditne kartice), koje tada neće biti moguće slati preko weba, e-maila ili instant messaging programa (tzv. instant-poruka).

**NAPOMENA:** Private Data Protection ne može štiti vaše osobne podatke dok ih ne definirate. Više informacija potražite na Online Help pod **Guarding against Internet Attacks > Protecting Private Data**.

**Provjerite je li Private Data Protection uključen:**

- u glavnom prozoru kliknite na **Network Control >Private Data Protection**
- provjerite je li **Enable Private Data Protection** označen
- kliknite na **Apply**.

**Dodajte ili promijenite Private Data Protection stavku:**

1. u glavnom prozoru kliknite na **Network Control >Private Data Protection**
2. provjerite je li **Enable Private Data Protection** označen

3. ako želite...
  - ...dodati novu stavku, kliknite na **Add**
  - ...promijeniti postojeću stavku, označite ju, pa kliknite na **Edit**
4. upišite ime i opis u **Item Name** i **Description** polje
5. upišite svoje osobne podatke u **Data** polje. PC-cillin Internet Security usporedit će podatke točno onako kako ih napišete. Podaci koje upišete su case-sensitiv (osjetljivi na veličinu slova) pa se, primjerice, trend, TREND i tReNd smatraju različitim pojmovima.
6. odaberite jedno ili više od sljedećega:
  - kako biste spriječili slanje tog privatnog podatka putem weba, označite **Check Web Protocol**
  - kako biste spriječili slanje tog privatnog podatka putem e-maila, označite **Check Mail Protocol**
  - kako biste spriječili slanje tog privatnog podatka preko instant messaging programa, označite **Check Instant Messenger Protocol**
7. kliknite na **OK**
8. kliknite na **Apply**. Stavka je spremljena.

## 3.10. Anti-spam

Spam e-mail (poznat kao junk email, engl. junk=smeće), osim što je iritantan problem za korisnika, predstavlja i izvor povećanih troškova bandwidtha. PC-cillin Internet Security Anti-spam funkcija identificira spam e-mail poruke i dodaje u njihovo zaglavlje oznaku tako da mogu biti lako identificirane i filtrirane.

Omogućite da Anti-spam filtrira vaše e-mail poruke.

### Potvrdite da je Anti-spam omogućen:

- u glavnom prozoru PC-cillin Internet Security kliknite na **Email > Anti-spam**
- provjerite je li **Enable Anti-spam** označen.

Možete podesiti PC-cillin Internet Security Anti-spam da radi na tri različita nivoa. Na najvišem nivou anti-spam pravila veoma su stroga, kako bi što više spam e-mail poruka bilo pravilno označeno, međutim, povećava se mogućnost da legitiman e-mail bude pogrešno označen kao spam. Najniži nivo ima mnogo opuštenija anti-spam pravila. To znači da neke spam e-mail poruke neće biti označene kao spam., ali je manja mogućnost da će legitiman e-mail biti pogrešno označen kao spam.

Kada je e-mail poruka prepoznata kao spam, na početku retka Subject dodaje se oznaka "SPAM". Namjestite pravilo u vašem e-mail programu da filtrira te poruke u posebnu, SPAM mapu, tako da možete povremeno provjeravati nalazi li se u njoj neka legitimna e-mail poruka (provjerite dokumentaciju svojeg e-mail klijenta za više informacija o podešavanju pravila filtriranja).

Anti-spam također ima Approved Senders List (popis odobrenih pošiljatelja) i Blocked Senders List (popis blokiranih pošiljatelja).

Bilo koja e-mail poruka poslana s adrese koja je navedena u Approved Senders List nikada neće biti označena kao spam. Bilo koja e-mail poruka poslana s adrese koja je navedena u Blocked Senders List uvijek će biti označena kao spam.

#### **Podesite Anti-spam postavke:**

- u glavnom prozoru kliknite na **Email > Anti-spam**
- označite **Enable Anti-spam**
- odaberite razinu zaštite na **Anti-spam Level** kliznoj traci
- ako želite dodati e-mail adresu na Approved ili Blocked Senders Listu, kliknite na **Edit Approved/Blocked Senders**
- pratite upute na ekranu koji će se pojaviti
- kliknite na **OK** i vratite se na početni Anti-spam ekran
- kliknite na **Apply**.

**NAPOMENA:** e-mail poruke veće od limita specificiranog u postavkama dolaznog e-maila neće biti kontrolirane za spam.

### **3.10.1. Anti-spam za Outlook™**

Trend Micro Anti-spam za Outlook također se nalazi na PC-cillin Internet Security CD-u. Ovaj osobni anti-spam alat instalira se kao dodatak u vaš Microsoft Outlook. Anti-spam za Outlook filtrira vaše e-mail poruka putem heurističke tehnologije, baze spam-uzoraka, kao i Approved i Blocked Senders Liste.

Anti-spam za Outlook nudi sljedeću funkcionalnost:

- moćan i prilagodljiv Anti-spam Engine ugrađen u osobni dodatak za Microsoft Outlook
- automatsko smještanje filtriranih poruka u "karantenu", radi kasnije analize
- korisnik određuje Approved Senders i Blocked Senders List
- izvještavanje o spamu i lažnoj detekciji
- statistike filtriranja za obrađene i e-maile u "karanteni"
- podrška za ručno i automatsko ažuriranje dijelova programa.

#### **Ako želite instalirati Anti-spam za Outlook:**

- ubacite Trend Micro PC-cillin Internet security CD u svoj CD-ROM uređaj
- ako se izbornik automatski pojavi, kliknite na **Install Anti-spam for Outlook**, te potom **Next**
- ako se izbornik ne pojavi automatski, iz Windows taskbara kliknite na **Start > Run**. U **Open** polje upišite D:\Antispam\setup.exe i kliknite na **OK**. (D:\ je oznaka vašeg CDR0M-a); kliknite na **Next**.
- kliknite na **Yes** da biste nastavili instalaciju Anti-spama za Outlook (instalacija će se prekinuti ako ne prihvatite uvjete).

**NAPOMENA:** kako bi se spriječilo nepotrebno trošenje računalnih resursa, Trend Micro preporučuje gašenje Anti-spam funkcije unutar PC-Cillin Internet Securitya kada koristite Anti-spam za Outlook.

## 4. Zaštita internetske veze

### 4.1. Osobni vatrozid (Personal Firewall)

PC-cillin Internet Security Personal Firewall štiti vaše računalo od napada s interneta. Firewall ili vatrozid je zapreka između vašeg računala i mreže (LAN ili internet). Ta zapreka pregledava i filtrira dolazni i odlazni mrežni promet. Filtriranjem prometa, vatrozid pomaže u sprečavanju hakerskih napada koji izazivaju štetu na računalu.

PC-cillin Internet Security Firewall pripada vrsti tzv. stateful inspection firewalle, što znači da prati i provjerava status svake veze kako bi se uvjerio u regularnost i legitimnost prometa. Takav firewall može detektirati odvija li se komunikacija, npr. preko porta 80, nekim drugim protokolom osim očekivanim HTTP-om. PC-cillin Firewall vodi računa o cijeloj sesiji, a ne samo o pojedinim IP paketima (osnovne jedinice za prijenos podataka preko mreže). Firewall koristi te informacije, kao i popis pravila, kako bi odredio hoće li određeni promet biti propušten ili blokiran.

Odluke o filtriranju ne temelje se isključivo na pravilima, nego i na kontekstu koji je određen prometom paketa koji su već prošli kroz vatrozid.

Osobni vatrozid uključuje sljedeće značajke:

- fleksibilnost pri kreiranju i primjeni različitih vatrozidnih profila, ovisno o okruženju
- dopustite, zabranite, upozorite na promet na specifičnom portu, protokolu ili aplikaciji
- kada koristite High Security Level, a određena aplikacija pokušava kontaktirati s internetom, javlja se upozorenje s pitanjem korisniku želi li dopustiti taj promet
- Intrusion Detection System (IDS) komponenta firewalle sprečava tipične napade na njega samoga (Too Big Fragment, Overlapping Fragment Attack, Tiny Fragment Attack itd.)
- zaustavlja trojance blokirajući portove za koje je poznato da se koriste prilikom napada
- ažuriranje firewall i IDS pravila
- sposobnost filtriranja HTTP stringova koji se koriste u komunikaciji između servera, što sprečava viruse kao što su NIMDA i Code Red
- automatska promjena profila, ako se promijeni mrežna okolina.

#### 4.1.1. Uključivanje osobnog vatrozida - firewalle

Uključite osobni vatrozid kako biste se mogli spojiti na internet ne razmišljajući o tome hoće li netko neovlašteno pristupiti vašem računalu. Osobni vatrozid vas štiti od hakera koji pokušavaju ukrasti datoteke, informacije ili jednostavno učiniti štetu u vašem računalu.

#### Potvrđivanje statusa osobnog vatrozida:

- u glavnom prozoru PC-Cillina kliknite na **Network Security > Personal Firewall**
- provjerite je li Firewall uključen, stavkom **Enable Personal Firewall**
- kliknite na **Apply** za potvrdu.

### 4.1.2. Osobni firewall-profil

Trend Micro PC Cillin Internet Security omogućuje vam konfiguraciju različitih firewall-profila za različite uvjete. Ovisno o vašim mrežnim postavkama, mogu vam zatrebati određeni servisi ili portovi za normalno funkcioniranje mreže. Korištenjem Personal Firewall profila možete lako mijenjati postavke između, primjerice, onih za kućno korištenje i Wireless (bežične) mreže, držeći sigurnost stalno na najvišoj razini. Personal Firewall dolazi konfiguriran za različite situacije. Te postavke možete mijenjati, koristiti bez izmjene ili kreirati svoje profile.

**Napomena:** za više informacija o kreiranju profila pogledajte online pomoć, dostupnu pod **Guarding Against Internet Attacks > Securing Internet Connections with Personal Firewall > Managing Personal Firewall**

## 4.2. Zaustavljanje internetskog prometa

Kompletna kontrola nad vašim internetskim prometom od vitalne je važnosti pri zaustavljanju virusa i/ili drugih oblika neovlaštenog pristupa. Emergency Lock opcija zaustavlja sav dolazni i odlazni promet i korisna je za slučajeve neovlaštenog pristupa računalu ili prilikom epidemije virusa.

#### Aktivacija Emergency Lock opcije:

- u glavnom prozoru kliknite na **Summary > Internet Security Status**, a potom **Halt Internet Traffic!** Time ste prekinuli sav internetski promet, tako da nećete biti u mogućnosti koristiti web ili provjeravati mail dok ne deaktivirate Emergency Lock.

#### Deaktivacija Emergency Lock opcije:

- kliknite na ponovno **Halt Internet Traffic**.

**Savjet:** u Windows trayu desnom tipkom miša kliknite na na PC-Cillin Internet Security ikonu i odaberite **Halt Internet Traffic**, ili - kad Real-time Scan otkrije virus - kliknite na **Halt Internet Traffic** u poruci koja se pojavi.

## 4.3. Blokiranje mrežnih virusa

Mrežni virusi, poput NIMDE, brzo se šire preko interneta i lokalnih mreža. Trend Micro PC-Cillin Internet Security pomaže vam da se zaštitite od infekcije, i sprečava vaše računalo da

zarazi druga računala. Nakon što detektira mrežni virus, PC-Cillin Internet Security može poduzeti sljedeće korake:

- zaustaviti kompletan internetski promet
- obavijestiti korisnika pop-up prozorom (Red Alert poruka).

**Kako biste dobili informacije o mrežnim virusima, napravite sljedeće:**

1. u PC-Cillin Internet Security glavnom prozoru kliknite na **Network Security > Network Virus Emergency Center**
2. kliknite na link (poveznicu) za više informacija o pojedinom virusu.

**Za promjenu postavki napravite sljedeće:**

1. u PC-Cillin Internet Security glavnom prozoru kliknite na **Network Security > Network Virus Emergency Center**
2. odaberite jedno
  - za zaustavljanje potpunog internetskog prometa prilikom detekcije mrežnog virusa kliknite na **Halt all Internet Traffic when Network Virus Detected**
  - za prikazivanje obavijesti o opasnosti odaberite opciju **Display Red Alert Pop-up**
3. kliknite na **Apply**.

## 4.4. Filtriranje neprikladnog web-sadržaja

Za zaštitu od neprikladnog web-sadržaja, Trend Micro PC-Cillin Internet Security nudi vam URL Filter funkciju. Ova vam opcija dopušta definiranje web-stranica koje želite zabraniti korisnicima.

URL Filter funkcionira u sljedećim načinima rada:

- zabranjuje pristup svim web-stranicama, a korisnik tada definira stranice kojima želi dopustiti pristup – popis dopuštenih stranica poznat je kao **Approved URLs List**
- dopušta pristup svim web-stranicama, a korisnik tada definira stranice kojima NE ŽELI dopustiti pristup – ovaj popis poznat je kao **Blocked URLs List**
- dopušta pristup svim web-stranicama, osim onih definiranih u pojedinim unaprijed zadanim kategorijama. Te kategorije formira i ažurira Trend Micro.

**Za filtriranje neželjenog web-sadržaja napravite sljedeće:**

1. u PC-cillin Internet Security glavnom prozoru kliknite na **Network Control > URL Filter**
2. odaberite **Enable URL Filtering**
3. odaberite željenu akciju za filtriranje
4. kliknite na **Apply**.

Prilikom pristupa nedopuštenim web-stranicama na ekranu će se pojaviti obavijest o zabrani.

**Za dodavanje ili izmjenu popisa iznimaka napravite sljedeće:**

1. u PC-cillin Internet Security glavnom prozoru kliknite na **Network Control > URL Filter**
2. provjerite je li uključena opcija **Enable URL Filtering**
3. odaberite jedno
  - za dodavanje ili izmjenu zabranjenih stranica kliknite na **Block access to...** i popis blokiranih stranica bit će u funkciji

- za dodavanje ili izmjenu dopuštenih stranica kliknite na **Allow access to...** i popis dopuštenih stranica bit će u funkciji
4. kliknite na **View Exceptions**
  5. napravite jedno
    - **za dodavanje web-stranica:**
      - a) kliknite na **Add**
      - b) na **Add/Edit Site** prozoru odaberite **Add URL** i unesite adresu, ili - za unos adresa izravno iz Internet Explorer cachea - odaberite **Import Recently Accessed URLs** te odaberite adresu ili više njih za unos
      - c) opcionalno, kliknite na **Include all Sub-pages under these URLs**, što će dodati sve podstranice određenog web sitea na popis (primjerice, ako ste dodali [www.nekastranica.com](http://www.nekastranica.com), ova opcija će dopustiti ili blokirati pristup [www.nekastranica.com/stranica1](http://www.nekastranica.com/stranica1) ili [www.nekastranica.com/stranica2](http://www.nekastranica.com/stranica2))
      - d) kliknite na **OK** za povratak na glavni **URL Filtering** prozor
    - **za izmjenu web-stranica:**
      - a) izaberite adresu koju želite izmijeniti
      - b) kliknite na **Edit**
      - c) na **Add/Edit** site prozoru izmijenite traženu adresu
      - d) kliknite na **OK** za povratak na glavni **URL Filtering** prozor
    - **za brisanje web-stranica:**
      - a) izaberite URL (ili više njih) koje želite izbrisati
      - b) kliknite na **Delete**
  6. kliknite na **OK** da se vratite na glavni **URL Filtering** prozor
  7. kliknite na **Apply**.

#### 4.4.1. Blokiranje unaprijed zadanih web-kategorija

Trend Micro PC-cillin Internet Security može blokirati stranice na temelju kategorija koje izaberete. Dostupne kategorije su:

- Adult
- Sex
- Alcohol/Tobacco
- Illegal Drugs
- Gambling
- Crime
- Violence/Hate/Racism
- Hacking/Proxy Avoidance
- Cult/Occult
- Weapons/Military
- Games
- Web Communications
- Personal/Dating
- Chat/Instant Messaging
- Email
- Newsgroups
- Shopping/Auctions

- Software Downloads
- Streaming Media/MP3
- Job Search

## 5. Virusi

Pojednostavljeno, računalni virus je program koji se replicira. Kako bi to napravio, dodaje se drugom programu (npr. .exe, .com, .dll) i izvršava se svaki put kad i "program domaćin". Uz to, virusi često imaju i drugu namjenu - a to je da uzrokuju štetu.

Razorna komponenta virusa može biti brisanje važnih podataka na vašem hard disku ili npr. mijesanje brojeva u Excel tablicama, pa sve do ometanja u radu zvukovima, "iskakajućim" prozorima itd.

Ako želite znati više o virusima, možete posjetiti Trend Micro online Virusnu enciklopediju na web-stranici [www.trendmicro.com](http://www.trendmicro.com)

### 5.1. Što učiniti kada se detektira virus na vašem računalu?

Prvo, **ne paničarite!** Kada Trend Micro PC-cillin Internet Security pronađe virus uz pomoć *Real-time*, ručne (Manual Scan) ili e-mail (Mail Scan) provjere, obavještava vas da je virus detektiran.

Kod *Real-time* i *Mail Scan* provjere prikazuje se poruka koja opisuje zaraženu datoteku i poduzetu akciju (*Scan Action*).

Poduzete akcije za *Real-time*, Manual ili Mail Scan ovise o postavkama konfiguriranim za svaku vrstu provjere. Međutim, unaprijed zadana vrijednost za sve provjere je *Clean* (čisti).

Ako se pokaže da je datoteka zaražena, PC-cillin Internet Security prvo ju pokušava očistiti. Druga, tj. alternativna akcija za *Real-time* i *Manual Scan* je *Quarantine* (staviti u karantenu).

PC-cillin Internet Security može prepoznati zlonamjerne programe koji ne mogu biti očišćeni. Neki zlonamjerni programi (kao trojanci i crvi) ne mogu zaraziti datoteke, i zbog toga po definiciji ne mogu biti očišćeni. Također, neke vrste virusa prebrišu postojeće podatke, što čišćenje čini nemogućim. Zbog toga poruka *Clean failed* u log-zapisima ne znači nužno da virus nije uspješno uklonjen. Podrazumijeva se, PC-cillin Internet Security premješta datoteke koje nije sposoban očistiti u Quarantine mapu.

### 5.2. Akcije s datotekama koje nije moguće očistiti

Zlonamjerni programi u karanteni ne mogu biti očišćeni, s obzirom na to da su oni programi. Virus nije zarazio datoteku, nego cijeli program zahtijeva čišćenje. Obrišite sve zlonamjerne programe u karanteni.

Za više informacija o postupanju s datotekama u karanteni pogledajte interaktivni **Vodič za karantenu (Quarantine Guide)**:

- u glavnom prozoru kliknite na **System > Quarantine**
- kliknite na **View Quarantine Guide** i slijedite upute.

Možete naučiti vrste virusa pregledom log-zapisa. Sljedeća tablica objašnjava kako identificirati različite vrste virusa i ostalih prijetnji prema njihovom imenu:

vrsta	oznaka	primjer
trojanski konji	TROJ_<ime>	TROJ_QAZ.A
crvi	WORM_<ime>	WORM_KLEZ
skriptni virusi	VBS_<ime> JS_<ime>	VBS_BRITNEYPIC.A
virusi koji zaraze datoteke	PE_<ime>	PE_VETIKINS.A
spyware	SPYW_<ime>	SPYW_NARGON.A

### 5.3. Čišćenje boot-virusa

Boot sektor virusi posebno su problematični (i opasni) jer zauzimaju osjetljivi dio hard diska, tzv. *Boot Sector*, i učitavaju se u memoriju računala svaki put kada se računalo upali. Iz memorije, lako se šire na bilo koju datoteku koja je naknadno otvorena, kao i na diskete koje se koriste.

PC-cillin Internet Security automatski provjerava prisutnost boot-sektor virusa prilikom ručne ili unaprijed zakazane provjere (Manual Scan, Scheduled Scan). Ako ga pronađe, PC-cillin Internet Security poduzima radnju definiranu/zadanu za tu vrstu provjere.

**NAPOMENA:** Boot-virusi se lako šire, pa ako PC-cillin Internet Security detektira takav virus, vrlo je lako moguće da je jedna ili više disketa također zaražena. Pokrenite unaprijed zadani task *Floppy Scan* za svaku disketu.

## 6. Podrška

Ako imate pitanja o korištenju usluge SURFAJTE SIGURNO, odnosno programa PC-cillin, kontaktirajte Službu za korisnike na besplatni telefon **0800 9000**, fax 0800 9009 ili e-mail kontakt@t-com.hr

U slučaju tehničkog pitanja, molimo vas da pružite što više informacija:

- serijski broj proizvoda
- verzija Trend Micro PC Cillin Internet Securitya, verzija Scan Enginea, verzija Patterna
- operativni sustav, ime, verzija i vrsta veze na internet
- točan tekst poruke o grešci
- koraci za repliciranje problema

### Prije kontaktiranja tehničke podrške

**Provjerite dokumentaciju:** vodič za korisnike i online pomoć nude iscrpne informacije o Trend Micro PC-cillin Internet Security proizvodu. Pregledajte oba dokumenta kako biste provjerili sadržavaju li odgovore na vaša pitanja.

**Posjetite Technical Support stranice** Trend Micra namijenjene tehničkoj podršci koje sadrže najnovije informacije o Trend Micro proizvodima. Naći ćete mnoga pitanja na koja su već dani odgovori.

**Za posjet Technical Support stranicama učinite sljedeće:**

- na glavnom prozoru kliknite na **Help > Technical Support Home Page**

### Posjet Trend Micro Customer Care centru

Trend Micro Customer Care centar sadrži najnovije informacije o Trend Micro PC-cillin Internet Securityu. Kao registrirani korisnik možete pristupiti informacijama koje nisu dostupne izvan ovih stranica.

Kako do Customer Care stranica:

- na glavnom prozoru kliknite na **Help > Customer Care Center**

### Prijava zaraženih datoteka Trend Micru

Svoje zaražene datoteke možete putem weba poslati na analizu u Trend Micro. Točnije, ako imate datoteku za koju sumnjate da je inficirana, a naš Scan Engine ne detektira virus ili ga ne može očistiti, pošaljite istu na:

<http://subwiz.trendmicro.com>

Molimo vas, uključite i kratki tekstualni opis simptoma koji se pojavljuju. Trend Micro inženjeri obradit će datoteku kako bi analizirali sadrži li virus(e) te vam je vratiti očišćenu – obično unutar 48 sati.