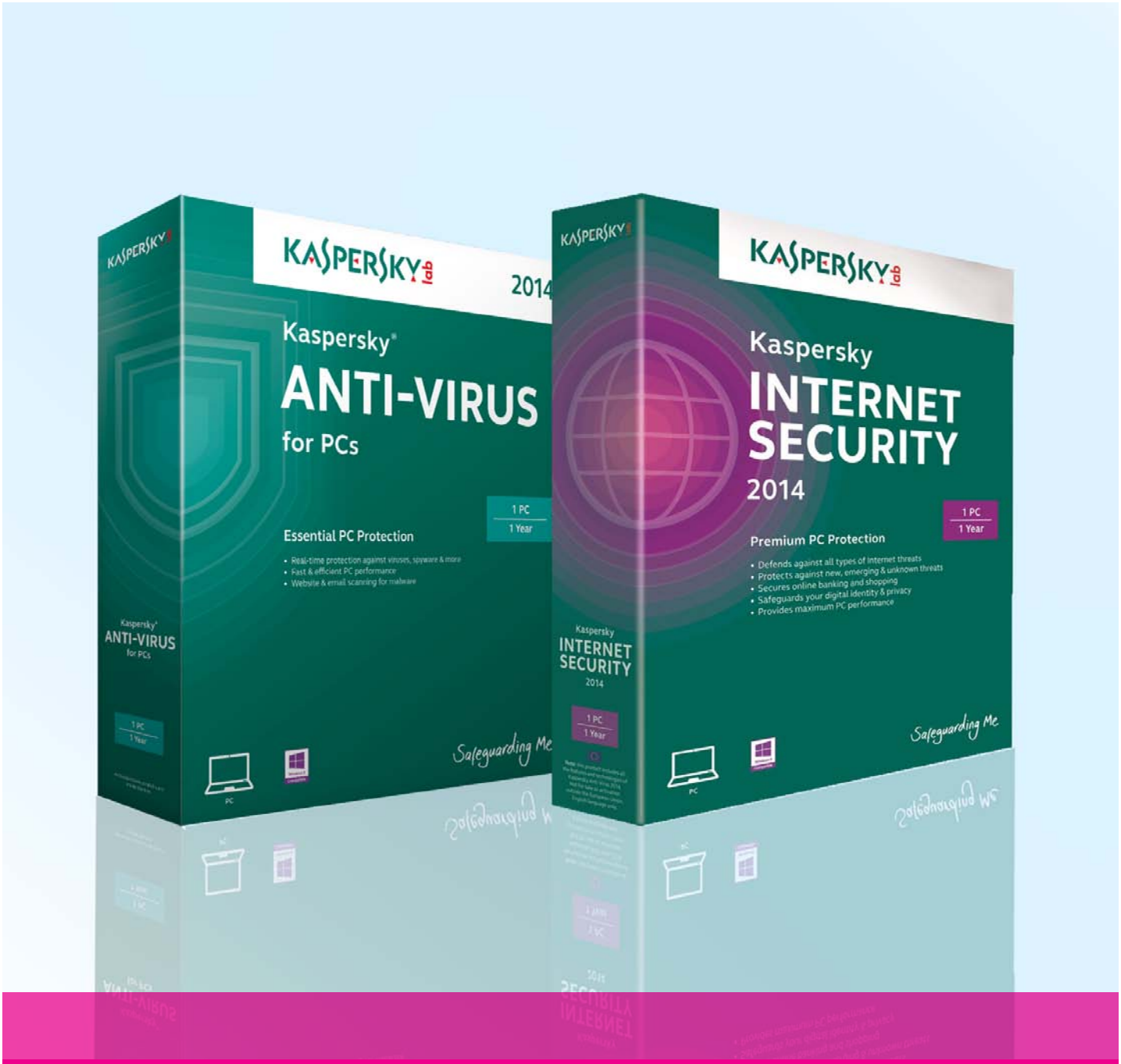

УПАТСТВО ЗА КОРИСТЕЊЕ НА KASPERSKY INTERNET SECURITY И KASPERSKY ANTI-VIRUS.

СПОДЕЛИ ДОЖИВУВАЊА

СОДРЖИНА

ИНСТАЛАЦИЈА И ПОДДРШКА

П: Како да го активирам и инсталирам софтверот KIS (Kaspersky Internet Security) или KAV (Kaspersky Anti-Virus)?
О: Потребно е најпрво да го одберете пакетот кој сакате да го активирате (KIS или KAV) и задолжително да ги прочитате и прифатите Општите услови за користење на пакетите. За потврда на активацијата потребен ви е Активирачкиот код, кој можете да го креирате сами веднаш по Вашата најава на Мој Телеком. Штом го активирате пакетот потребно е во делот Активни пакети (Онлајн софтверски пакети –>Активни пакети) да кликнете на линкот за соодветниот пакет и во прозорчето за инсталација на софтверот одберете го копчето Save или Run за да започнете со симнување на софтверот. Штом симнувањето на софтверот ќе заврши во Downloads, кликнете два пати на документот кој го симнавте или пак директно кликнете на копчето Run. Во прозорчето кое ќе се појави започнете со инсталацијата преку копчето Install и следете ги инструкциите. ПИН кодот на софтверот секогаш ќе можете да го видите на Мој Телеком (Онлајн софтверски пакети –>Активни пакети).

П: Ако инсталирам KIS дали треба да инсталирам и KAV?
О: Kaspersky Internet Security содржи сè што може да се најде во Kaspersky Anti-Virus.

П: Кој производ е вистинскиот за мене – KIS или KAV?
О: Во прилог се дадени главните функционалности на двата софтвери. Како насока, Kaspersky Lab го препорачува KIS за корисниците кои се често на Интернет бидејќи тој обезбедува врвна заштита. Неговиот најсовремен, хибриден приод кон дигиталната безбедност комбинира иновативни технологии базирани на „cloud“ со напредна антивирусна заштита за обезбедување на ефикасна безбедност во текот на онлајн активностите како што се сурфање, банкарство, комуникации и сл. KAV се препорачува за корисниците кои не се често на Интернет и нуди основна заштита за компјутерите.

Kaspersky Anti-Virus клучни функционалности:

- Следач на системот (System watcher)
  Дури и ако непознат злонамерен софтвер успее да влезе во вашиот компјутер, уникатниот System Watcher на Kaspersky ќе го открие опасното однесување и ќе ви овозможи да вратите или да поништите најголем дел од злонамерните активности.
- Подобра заштита против кражба на идентитет
  Новата алатка за заштита против кражба на идентитет ја подобрува вашата одбрана од обидите на интернет измамниците да добијат пристап до вашите лични информации.
- Automatic Exploit Prevention (автоматско спречување на експлоатација)
  Дури и ако вашиот компјутер и апликациите што функционираат на него не се ажурирани со најновите поправки, Kaspersky Anti-Virus може да спречи злоупотреба на ранливите точки со:
    - Контрола на стартување на извршни фајлови од апликациите со ранливи точки
    - Анализа на однесувањето на извршните фајлови за какви било сличности со злонамерни програми
    - Ограничување на активностите коишто се дозволени од апликациите со ранливи точки
- Минимално влијание на перформансите на компјутерот за голем број на сценарија за користење
  Kaspersky Anti-Virus е оптимизиран така што нема значително влијание на мрежната активност, инсталирањето на програмите, стартувањето на мрежните пребарувачи или стартувањето на програмите. Освен тоа, опцијата Gamer Mode овозможува непрекинато искуство во играњето на игри – при што сте заштитени.
- Оптимизирани антивирусни бази на податоци
  Со антивирусните информации обезбедени од Cloud, значително се намалени антивирусните бази на податоци складирани на вашиот компјутер – што ви помага да ги подобрите перформансите и да го намалите времето потребно за инсталација и ажурирање.
- Намалено трошење на батеријата
  Кога се инсталира на лаптоп којшто работи на батерија, Kaspersky Anti-Virus автоматски го намалува користењето на ресурсите – за да се зголеми времето на работење на лаптопот пред да треба да се наполни.
- Интерфејс лесен за користење
  Главниот прозорец на интерфејсот е оптимизиран за да ги подобри перформансите и за лесно користење за многу популарни кориснички сценарија, како стартување на проверки и решавање на проблеми.
- Виртуелна тастатура
  Виртуелната тастатура ви овозможува да ги внесете вашите банкарски информации онлајн преку кликања на маусот – така што вашите лични информации не можат да ги следат или да ги украдат keylogger-и, хакери или крадци на идентитет.

Kaspersky Internet Security клучни функционалности:

- Safe Money додава уште поголема сигурност при онлајн банкарство и шопинг
  Kaspersky Internet Security секогаш обезбедувал заштита на онлајн трансакциите, а со последната верзија, кога и да се обидете да се пријавите на страна за онлајн банкарство, страна за системи за плаќање или страна за е-трговија, нашата нова уникатна Safe Money функционалност:
    - Ќе го спореди URL на веб страната со база на податоци со безбедни страни
    - Ќе го провери сертификатот којшто се користи за воспоставување на безбедна конекција – за да се избегне скриено префрлање од вашата наменета страна до 'лажна' страна
    - Ќе провери дали вашиот систем има ранливи точки за онлајн банкарство поврзани со оперативниот систем на вашиот компјутер
    - Автоматски ќе предлага отворање на страната во Safe Money режим на работа – за дополнителна заштита од кражба на лични и финансиски податоци

  ... така што напредните технологии на Kaspersky секогаш Ве заштитуваат кога сте онлајн - шопинг, банкарство и друго.
- Безбедносната тастатура ги заштитува личните податоци што ги внесувате преку вашата тастатура
  Бидејќи keylogger-ите можат да ги копираат отчукувањата на тастатурата при внесувањето на бројот на вашата кредитна картичка или други вредни информации внесени преку вашата тастатура, Kaspersky Internet Security ја вклучува новата технологија Безбедносна тастатура. Кога отворате веб страна на банка или веб страна за плаќање – или кога внесувате лозинка на која било веб страна – Безбедносната тастатура се отвора автоматски за да ги заштити вашите податоци од keylogger-ите.
- Следач на системот (System watcher)
  Дури и ако непознат злонамерен софтвер успее да влезе во вашиот компјутер, уникатниот System Watcher на Kaspersky ќе го открие опасното однесување и ќе ви овозможи да вратите или поништите најголем дел од злонамерните активности.
- Подобрена функционалност за Родителската контрола
  Новата функционалност Родителска контрола вклучува нова и подобрена заштита за деца коишто го користат вашиот компјутер. Kaspersky Internet Security овозможува поефективна контрола на користењето на компјутерот и интернетот од страна на децата и овозможува посигурно филтрирање на веб страните коишто содржат несоодветна содржина.
- Нов анти-спам модул
  Kaspersky Internet Security вклучува нов, подобрен анти-спам модул којшто обезбедува посигурно филтрирање на несакани пораки и исто така вклучува подобрено известување за откриен спам.
- Подобра заштита против кражба на идентитет
  Новата алатка за заштита против кражба на идентитет ја подобрува вашата одбрана од обидите на интернет измамниците да добијат пристап до вашите лични информации.
- Automatic Exploit Prevention (автоматско спречување на експлоатација)
  Дури и ако вашиот компјутер и апликациите што функционираат на него не се ажурирани со најновите поправки, Kaspersky Internet Security може да спречи злоупотреба на ранливите точки с:
    - Контрола на стартување на извршни фајлови од апликациите со ранливи точки
    - Анализа на однесувањето на извршните фајлови за какви било сличности со злонамерни програми
    - Ограничување на активностите коишто се дозволени од апликациите со ранливи точки
- Минимално влијание на перформансите на компјутерот за голем број на сценарија за користење
  Kaspersky Internet Security е оптимизиран така што нема значително влијание на мрежната активност, инсталирањето на програмите, стартувањето на мрежните пребарувачи или стартувањето на програмите. Освен тоа, опцијата Gamer Mode овозможува непрекинато искуство во играњето на игри – при што сте заштитени.
- Оптимизирани антивирусни бази на податоци
  Со антивирусните информации обезбедени од Cloud, значително се намалени антивирусните бази на податоци складирани на вашиот компјутер – што ви помага да ги подобрите перформансите и да го намалите времето потребно за инсталација и ажурирање.
- Намалено трошење на батеријата
  Кога се инсталира на лаптоп којшто работи на батерија, Kaspersky Internet Security автоматски го намалува користењето на ресурсите – за да се зголеми времето на работење на лаптопот пред да треба да се наполни.
- Интерфејс лесен за користење
  Главниот прозорец на интерфејсот е оптимизиран за да ги подобри перформансите и за лесно користење за многу популарни кориснички сценарија, како стартување на проверки и решавање на проблеми.
- Брзо стартување на Виртуелна тастатура
  Виртуелната тастатура ви овозможува да ги внесете вашите банкарски информации онлајн преку кликања на маусот – така што вашите лични информации не можат да ги следат или да ги украдат keylogger-и, хакери или крадци на идентитет. Сега Kaspersky Internet Security овозможува брз пристап до Виртуелната тастатура директно од мрежните пребарувачи.

П: Дали треба да ги отстранам антивирус производите од трети лица пред да ги инсталирам производите на Kaspersky Lab?
О: Се препорачува да немате инсталирани антивирусни производи од трети лица на вашиот компјутер со цел да се избегнат проблеми со компатибилноста. KAV и KIS автоматски ќе отстранат некои антивирусни производи од трети лица коишто се инсталирани на вашиот компјутер во текот на процесот на инсталирање. Базата на податоци за некомпатибилен софтвер редовно се ажурира за да ги земе предвид новите верзии на производите на трети лица. Сепак, понекогаш базата на знаење за техничка поддршка ќе биде некој чекор понапред од алатката за автоматско отстранување, така што ако наидете на проблеми ве молиме да ја погледнете веб страницата на Kaspersky Lab.

П: Зошто web installer креира shortcut на мојот десктоп?
О: Се креира shortcut на десктоп за да се олесни активирањето на софтверот. Без ова беше тешко да се најде начин да се активира интерфејсот на софтверот. Кога се инсталира KIS се креира и shortcut до Safe Money за истата цел.

П: Дали можам да инсталирам KIS или KAV на компјутер што е веќе заразен?
О: Нормално да, но некои злонамерни софтвери (malware) конкретно се обидуваат да го деактивираат софтверот за заштита или да го спречат да се инсталира. Доколку инсталацијата не успее автоматски се стартува Kaspersky AVP алатката. Ова ќе направи длабинско чистење на вашиот систем што ќе го подготви Вашиот систем за целосна инсталација.

П: Каде можам да добијам поддршка за KIS и KAV?
О: Партнери кои го обезбедуваат пакетот се Македонски Телеком, КабТел и Kaspersky Lab и тие ви нудат широки можности за поддршка вклучувајќи:

- Отворени телефонски линии за техничка поддршка 24/7 на бројот 122
  База на знаење достапна на: support.kaspersky.com, којашто содржи детални одговори на прашања поврзани со инсталирањето, конфигурирањето и користењето на производите на Kaspersky Lab.
- Форумот на: http://forum.kaspersky.com

ЛИЦЕНЦИРАЊЕ НА СОФТВЕРОТ

П: Дали можам да го користам KAV/KIS софтверот бесплатно во одреден пробен период за да се уверам во неговите функционалности?
О: Да, секој нов корисник на KAV/KIS ќе добие 90-дена бесплатен пробен период за првиот активиран пакет за да се увери во неговите функционалности.

П: Што ќе се случи кога ќе истече бесплатниот период за користење на софтверот?
О: Доколку не го деактивирате софтверот во текот на бесплатниот период за користење, автоматски ќе започне наплатата на месечно ниво со цени дефинирани за активираниот пакет.

П: Дали во рамките на бесплатниот период можам да го активирам најпрвин KAV софтверот, а потоа KIS софтверот, со цел да ги испробам и двата типа на функционалности?
О: Да, во текот на бесплатниот период можете еднаш да го замените софтверот кој веќе сте го активирале. Замената се прави во делот на Активни пакети (Онлајн софтверски пакети -> Активни пакети) со одбирање на опцијата “Промени“ покрај активираниот пакет кој сакате да го промените. Потоа следи активација на пакетот на истиот начин како и иницијалната активација со внесување на Активирачки код. За последниот тип на софтвер кој е активен на вашиот уред по истекувањето на бесплатниот период ќе започне месечната наплата.

П: Дали ПИН кодот на софтверот KIS е компатибилен со ПИН кодот на софтверот KAV?
О: Не, не е. ПИН кодот е уникатен код за секој пакет.

П: Ако го заменам компјутерот дали можам да ја заменам и мојата копија на KIS или KAV на мојот нов компјутер?
О: Да, но ве молиме да имате предвид дека е легално да работите со KIS или KAV на онолку компјутери за колку што сте купиле лиценци.

ПРОАКТИВНА ЗАШТИТА ОД НЕПОЗНАТИ ЗАКАНИ

П: Како KAV или KIS го штити мојот компјутер од нови или непознати закани?
О: Околу 125.000 нови злонамерни програми се појавуваат секој ден. Откривањето на сите овие програми со користење на традиционална анализа на потпис е невозможно. Од оваа причина, проактивната заштита е основна средство на одбрана. KAV и KIS вклучуваат значително подобрена System Watcher технологија којашто ги следи и ги запишува активностите на сите апликации во системот, го споредува нивното однесување во однос на обрасците на злонамерна активност и ги блокира сите несакани активности. Ова значително ја зголемува стапката на откривање на нови и непознати закани.

П: Кои злонамерни активности можам да ги поништам?
О: Можете безбедно да поништите злонамерни промени направени од злонамерен софтвер на вашиот компјутер и да бидете сигурни дека вашиот систем не е загрозен. Можете да ги поништите следниве активности: активности со фајлови (креирање, преименување, менување, бришење на фајлови), активности на регистри (креирање, менување или бришење на клучни вредности на регистри), системски активности (стартување и запирање на процеси, вметнување во други процеси). Со тоа се прекинуваат и процесите што се започнати од страна на злонамерен софтвер и се ограничуваат мрежните конекции. Исто така, можете да ја утврдите големината на просторот (обично, 30 MB) на хард дискот за чување на историјата на активноста на програмот што е потребна за поништување на активностите на злонамерниот софтвер.

П: Што се Duqu Trojan и слични закани?
О: Главна цел на Duqu и сличен злонамерен софтвер е незабележено да се инсталира на системот и да краде лични податоци. Понатаму, таквиот злонамерен софтвер не само што може да краде лични податоци, туку може да предизвика и целосен пад на системот. Duqu вметнува

злонамерен код во системските процеси, честопати при активирањето на системот (односно пред антивирус програмата да почне да работи).
П: Како програмата ќе ме заштити од Duqu Trojan и слични закани?
О: За справување со овој вид на злонамерен софтвер, KAV/KIS го блокира упадот на закани слични на Duqu; софтверот не дозволува клучните делови од кодот да се имплементираат, со нивно ефикасно неутрализирање.

CLOUD ЗАШТИТА

П: Што е заштита базирана на "cloud" и зошто ми е потребна?
О: Важноста на заштитата базирана на "cloud" се зголемува секој ден бидејќи бројот на закани расте екстремно брзо. Главна предност на користењето на "cloud" технологија е тоа што таа нуди дури и побрза заштита од новите закани. Исто така, комбинацијата на технологии базирани на "cloud" со традиционалните методи на потпис му дава на вашиот компјутер високо ниво на заштита од сите различни видови на закани.

П: Што е безбедносна мрежа на Kaspersky?
О: Безбедносната мрежа на Kaspersky обединува милиони корисници ширум светот за брзо откривање на нови закани и утврдување на репутацијата на програмите и на веб страниците. Таа исто така ги вклучува и најновите технологии на Kaspersky Lab за заштита во реално време како што се Системот за итно откривање (UDS) и база на податоци за безбедни програми, фајлови и сл.

П: Ако не се сложам да учествувам во безбедносната мрежа на Kaspersky, можам ли да изберам да се придружам подоцна?
О: Да, има опција во менито којашто ви овозможува да го направите тоа. Треба да го изберете Feedback табот во подесувањата за софтверот и да го означите квадратчето со што потврдувате дека се согласувате да учествувате во безбедносната мрежа на Kaspersky.

П: Колку луѓе учествуваат во безбедносната мрежа на Kaspersky?
О: Има над 1 милион корисници кои испраќаат информации во реално време до аналитичарите на злонамерен софтвер на Kaspersky Lab. Оваа информација честопати се однесува на нови закани.

П: Какви се придобивките за мене ако се придружам на безбедносната мрежа на Kaspersky?
О: Придонесуваш кон една целосно анонимна услуга која му помага на Kaspersky Lab да ги разбере развојните закани. Ова му овозможува на Kaspersky Lab брзо да реагира на појавата на нови и непознати злонамерни програми и да ги додаде во ажурираната база на податоци. Kaspersky Lab исто така може да додаде нови видови спамови во базата на податоци за спамови и да ја сподели информацијата на глобално ниво. Дополнително, Kaspersky Lab може да ги анализира апликациите и програмите на вашиот систем за ранливости и да ги сподели со развојната заедница. Kaspersky Lab не ги собира, обработува или складира вашите лични податоци на кој било начин.

П: Ако се придружам на безбедносната мрежа на Kaspersky, какви информации се испраќаат од мојот компјутер до вашиот аналитичар?
О: Ние собираме само анонимни податоци – информација за оперативниот систем на којшто работите и за софтверот на вашиот компјутер и конкретни информации за кој било софтвер на вашиот компјутер којшто се однесува сомнително. Не се собираат лични податоци и нема начин како да се следат информациите назад до вашиот компјутер.

П: Јас не сум член на безбедносната мрежа на Kaspersky. Дали се уште ќе имам придобивки од брзата реакција на новите закани што ја нуди Системот за итно откривање (UDS)?
О: Да, сите корисници на Kaspersky Lab кога се онлајн ги користат придобивките од заштитата базирана на "cloud", вклучувајќи го и Системот за итно откривање (UDS).

П: Како да откријам дали е безбедно да се работи со програм кој е преземен од Интернет или од некој друг извор?
О: Ако сте преземале фајл од Интернет и не сте сигурни дали е безбеден, можете да ја проверите неговата репутација со користење на File Advisor функцијата. Главна придобивка од оваа функција е дека таа ги користи најновите информации од „cloud"-от. Тоа ви овозможува да проверите колку се безбедни некои релативно нови програми или фајлови, дури и пред тие да бидат внимателно анализирани од страна на специјалисти, благодарение на објектите што се доделуваат на одредено ниво на сигурност од други корисници. File Advisor во KAV/KIS сега овозможува да се провери потеклото на фајлот (односно дали дошол преку емаил, IM или URL).

П: Какви видови на фајлови можам да проверам со користење на File Advisor?
О: File Advisor може да се користи за да се провери репутацијата на извршните фајлови (.exe, .js, .vbs), командните фајлови (.bat, .cmd), регистерските фајлови (.reg) и неколку други видови на фајлови (.msi, .msc, .cpl, .dll).

AUTOMATIC EXPLOIT PREVENTION (АВТОМАТСКО СПРЕЧУВАЊЕ НА ЕКСПЛОАТАЦИЈА)

П: Што е exploit (експлоатација)?
О: Exploit (експлоатација) е злонамерна програма или дел од злонамерен код кој наоѓа ранливости кај популарни апликации како што се Adobe Reader, Internet Explorer, и Firefox и ја користи таа слаба точка за да се обиде и стекне контрола врз компјутерот, да ги украде вашите лични податоци и сл.

П: Како KAV/KIS ме штити од exploit-и (експлоатации)?
О: KAV/KIS вклучува нова технологија, Автоматско спречување на експлоатација (AEP) којашто ги спречува и ги блокира овие видови на

експлоатации. Поконкретно, ова вклучува:

- Контрола на стартување на извршните фајлови (вклучувајќи ги и веб пребарувачите) ако бидат откриени какви било ранливости или од апликации кои не биле наменети за активирање на извршни фајлови (Microsoft Word, Excel и сл.).
- Ако се активираат извршни фајлови, нивните активности се проверуваат за какви било знаци на exploit однесување.
- Контрола на сите активности што ги врши апликација во која е откриена ранливост (на пр. следење на линк, пишување на други процеси во меморија и сл.).

П: Дали сè уште треба да барам ранливости (Vulnarability Scan) сега кога новата технологија Автоматско спречување на експлоатација е вклучена во софтверот?
О: Да, се препорачува да барате и ранливости. Автоматското спречување на експлоатација ви помага да се заштитите од експлоатации кои ги искористуваат новите, неидентификувани ранливости. Vulnarability Scan бара ранливости кои веќе биле идентификувани од страна на добавувачите на софтвер (врз основа на базата на податоци обезбедена од Secunia). Во вториот случај софтверските компании веќе имаат издадено закрпи за ублажување на познатите ранливости и за да го спречат нивното искористување. Поради тоа, препорачуваме да се користат двете методи за обезбедување на целосна заштита на компјутерите.

БЕЗБЕДНО СУРФАЊЕ СО KASPERSKY : ANTI - PHISHING

П: Дали инсталирањето на Kaspersky Internet Security ќе ме спречи да пристапам до злонамерни интернет страници?
О: Kaspersky URL Advisor ќе ве заштити со тоа што ќе ве предупреди за линковите што водат до злонамерни или веб страни за крадење на идентитет, обележувајќи ги со боја која го покажува статусот на заштита на секој линк. Понатаму, можете да ја видите репутацијата и категоријата на секоја страница, вклучувајќи ги и сомнителните страни со несакана содржина (на пр. веб страни за крадење на идентитет, страници поврзани со насилство или дрога и сл.). Сепак, ако има одредени веб страници до кои би сакале да пристапите и покрај советите на Kaspersky Lab, можете да ги дефинирате како исклучоци и да пристапите до нив. Kaspersky Lab ви препорачува да го користите Safe Run режим на работа за да пристапите до ваквите веб страници.

П: Од каде Kaspersky Lab ги добива своите Anti-Phishing информации?
О: Kaspersky Lab користи голем број на извори за да ги идентификува заканите за крадење на идентитет. Ние во голема мера придонесуваме кон PhishTank услугата, која ја води OpenDNS, и која нуди консолидирана база на податоци за познати веб страни за крадење на идентитет којашто континуирано ја ажурира Open Source заедницата и обичните корисници. Ние исто така сме регистрирани на Anti-Phishing листи од главни финансиски институции и на меѓународната Anti-Phishing работна група, меѓу останатите.

П: Како производите на Kaspersky Lab ме штитат од крадење на идентитет?
О: KAV и KIS проактивно откриваат сомнителни веб страни за крадење на идентитет и ги анализираат информациите за секоја, на пример дали има некакви знаци во URL-то кои се индикативни дека станува збор за веб страна за крадење на идентитет. Доколку се откријат такви знаци, страната се обележува како веб страна за крадење на идентитет и пристапот до неа се блокира, дури и ако не е во базата на податоци на веб страни за крадење на идентитет.

БЕЗБЕДНО СУРФАЊЕ СО KASPERSKY : ANTI - SPAM

П: Како Kaspersky Lab идентификува спам?
О: Покрај традиционалните методи како што е анализа на текст и слики, KIS ги користи последните “cloud” технологии и хевристика за да ги заштити корисниците од спам, што значително ја зголемува ефикасноста на препознавањето на спамови. Заштитата од спамови преку “cloud” е лесна и сигурна бидејќи се одвива во реално време. Ова овозможува брзо и ефикасно идентификување и блокирање на нови спамови. Ние сме регистрирани на светските водечки бази на податоци за спамови со цел да осигуриме дека нашите корисници имаат одлична заштита од несакана електронска пошта.

БЕЗБЕДНО ФИНАНСИСКО РАБОТЕЊЕ: SAFE MONEY (БЕЗБЕДНИ ПАРИ)

П: Што претставува функционалноста Safe Money и зошто ми е потребна?
О: Safe Money го заштитува целото финансиско работење преку онлајн банкарство и системи за плаќање (на пр. PayPal, WebMoney и др.) и за време на онлајн шопинг со стартување на веб страната во безбеден режим на работа. KIS го ограничува начинот на којшто другите програми и процеси можат да пристапат до податоците коишто се пренесуваат во рамките на Safe Money режимот на работа што ви овозможува да се осигурате дека вашите лични податоци се заштитени од кражба.

П: Како функционира Safe Money?
О: Секогаш кога корисникот ќе влезе во онлајн банкарски систем, веб страна на банка или личен профил на систем за плаќање, KIS ги

извршува следниве активности:

- Потврдува дека барањето е испратено до оригиналната веб страна на банката или системот за плаќање (проверено во однос на листа на веб страни што може да се ажурира во рамките на софтверот).
- Го потврдува безбедносниот сертификат, за да се избегне пренасочување на лажна веб страна.
- Го скенира оперативниот систем за слабости коишто можат да бидат критични за онлајн банкарството.
- Нуди отворање на веб страната во Safe Money режим на работа за заштита на вашите лични податоци од кражба.

П: Како да пристапам до Safe Money модулот?
О: Можете да пристапите до Safe Money преку главниот прозорец или преку подесувањата. Исто така, Safe Money се активира кога ќе се обидете да пристапите на страни за е-банкарство, е-шопинг или системи за плаќање.

П: Ако страната на мојата банка не се отвора во безбедна средина, дали може да ја додадам на листата на веб страни коишто функционираат во безбеден режим на работа?
О: Да, можете да додавате веб страни на листата.

БЕЗБЕДНО ФИНАНСИСКО РАБОТЕЊЕ: SECURE KEYBOARD (БЕЗБЕДНОСНА ТАСТАТУРА)

Што е Secure Keyboard (Безбедносна тастатура)?
О: KAV/KIS вклучува функционалност за дополнителна заштита на личните податоци, дури и кога користите физичка тастатура. Ако отворите веб страна на банка или за плаќање или внесете лозинка на која било веб страна, Безбедносната тастатура ќе се активира автоматски. Подесувањата на софтверот ви овозможуваат да изберете и други категории на веб страни каде заштитниот режим на работа на Безбедносната тастатура треба да се активира.

П: Која е разликата помеѓу Secure Keyboard (Безбедностна тастатура) и Virtual Keyboard (Виртуелна тастатура)?
О: Виртуелната тастатура ги заштитува корисниците од поголем број закани и се препорачува нејзино користење при чувствителни финансиски трансакции. Меѓутоа, бидејќи таа треба да се стартува рачно, креиран е режим на работа на Безбедносна тастатура што се стартува автоматски. Само KIS ја има функцијата за брзо стартување преку Виртуелната тастатура (автоматски се активира во полето за внесување на податоци ако корисникот отвори страна за банкарство или плаќање). Оваа функционалност ја нема во KAV .

П: Дали да ја активирам функцијата Secure Keyboard (Безбедносна тастатура)?
О: Не мора да ја активирате рачно. Таа ќе се вклучи по првото стартување на компјутерот по инсталирањето на KIS .

БЕЗБЕДНО ФИНАНСИСКО РАБОТЕЊЕ: VIRTUAL KEYBOARD (ВИРТУЕЛНА ТАСТАТУРА)

П: Што ќе го спречи keylogger-от едноставно да ми ги следи кликовите со глувчето за да види што пишувам на Виртуелната тастатура?
О: Виртуелната тастатура користи специјална технологија за спречување на работата на стандардни и специјални софтвери за шпионирање на екрани или читање на логови кога таа се наоѓа на екранот.

П: Што ја прави Kaspersky Виртуелната тастатура подобра од стандардната тастатура на екран што ја добивам со Windows?
О: Тастатурата на екран на Windows е едноставно алтернативно средство за внесување на податоци, додека Виртуелната тастатура на Kaspersky Lab е специфично дизајнирана да се бори со техниките коишто ги користат сајбер криминалците при вршење злоупотреби во реалниот свет.

PARENTAL CONTROL (РОДИТЕЛСКА КОНТРОЛА)

П: Ако сакам да го контролирам користењето на компјутерот на моите деца, како можам да ги спречам да ги сменат подесувањата?
О: Можете да ги заштитите подесувањата со лозинка на секој компјутер со цел да спречите промена или отстранување на софтверот.
П: Како да го контролирам користењето на интернет на моето дете?
О: Можете да го контролирате времето коешто вашите деца го поминуваат на интернет со ограничување на бројот на часови коишто им се дозволени на интернет или со забрана на нивниот пристап во одредени периоди од денот. Исто така можете да поставите ограничување на преземањето на одредени типови на фајлови (видеа, архиви, апликации и др.) или да блокирате пристап до веб страни со несакана содржина (насилство, дрога, онлајн шопинг и др.)

П: Дали можам да ја контролирам активноста на моето дете на социјалните мрежи?
О: Да, можете едноставно да ја конфигурирате функцијата Parental Control (Родителска Контрола) за да видите со кого вашето дете комуницира, да ја забраните комуникацијата со одредени луѓе или да блокирате пристап до социјалните мрежи како што се MySpace, Twitter, Facebook.

П: Дали можат моите деца да видат кои текстуални низи се филтрирани?
О: Вашите деца не можат да видат кои текстуални низи се филтрирани. Ова е делумно бидејќи низите можат да содржат пцовки или некултурни изрази коишто можат да предизвикаат правни проблеми ако се прикажуваат на деца во одредени земји и бидејќи тие веројатно спаѓаат во фразите од коишто сакате да ги заштитите вашите деца. Исто така можете да внесете дополнителни низи за филтрирање.

П: Дали дополнителните низи што сум ги внел ќе бидат видливи за моите деца?
О: Не, дополнителните низи (клучни зборови) што сте ги внеле нема да бидат видливи за вашите деца под услов да поставите лозинка за пристап до управување со Parental Control (Родителска Контрола). Ако не поставите лозинка, тогаш секој ќе има пристап до правилата што сте ги поставиле и дури може да ја исклучи функцијата Parental Control (Родителска Контрола).

П: Што ќе се случи ако се детектира забранета низа?
О: Ако една забранета низа (клучни зборови) се детектира, тогаш тој податок ќе биде регистриран и подоцна ќе можете да ја видите статистиката на појавата на оваа низа во вашата домашна мрежа.
П: Дали можам да спречам моето дете да ги испраќа онлајн своите лични податоци?
О: Да, можете да дефинирате низи како што се вашата адреса, електронска пошта и телефонски броеви и да забраните нивно испраќање.

П: Кои апликации за испраќање брзи пораки можат да се контролираат?
О: Можете да ги контролирате Yahoo, MSN, Windows Live, ICQ, QIP, Miranda, AIM, SIM, Trillian, Jabber, Google Talk и други.

RESCUE DISK

П: Ако мојот компјутер се зарази со вирус, а оперативниот систем не се покренува, како Rescue Disk може да ми помогне?
О: Rescue Disk се базира на Linux фајл систем, а не Windows фајл систем, затоа е генерално отпорен на истите групи вируси. Како дел од процедурата за обновување, Rescue Disk ќе се обиде да воспостави конекција со интернет и да употреби контра мерки во реално време, ако се достапни.

ПРОВЕРКА НА РАНЛИВОСТА НА СИСТЕМОТ

П: Зошто проверката на ранливоста на системот е одделена од целосната проверка?
О: Ранливоста на системот не е повреда на безбедноста на вашиот компјутер, таа е само потенцијален недостаток на безбедноста на вашиот систем којшто сајбер криминалците можат да го злоупотребат за да добијат пристап до вашиот систем. Примарната придобивка од поделбата на овие функции е дека целосната проверка сега е многу побрза.
П: Kaspersky Internet Security и Kaspersky Anti-Virus не проверуваат ранливост како дел од проверката на критичните делови или целосна проверка – зошто е тоа така?
О: Ранливоста не е исто што и заразување со вируси. Справувањето со ранливоста на системот е напредна форма на проактивна одбрана. Исто така, отстранувањето на проверката на ранливост од целосната проверка и проверката на критичните делови значително ја зголемува брзината на проверка.
П: Што да правам со детектираната ранливост?
О: Сите проблеми детектирани во фазата на анализа на системот ќе бидат групирани според нивниот степен на опасност. Со цел да се елиминира ранливоста на системот, изберете ја ставката и кликнете на копчето „Fix it“ (Поправи).

ИНТЕЛИГЕНТНА ПРОВЕРКА СО ГОЛЕМА БРЗИНА

П: Како да спречам проверката да ми го забави компјутерот додека работам?
О: Постои опција проверката да започне само кога компјутерот не е во функција одреден временски период.

П: Зошто првата проверка трае многу подолго од наредните проверки?
О: Техниките на проверка на Kaspersky Lab вклучуваат неколку напредни техники на проверка за оптимизирање на следните проверки. Како пример можеме да го наведеме iChecker којшто ја отстранува потребата да се проверуваат фајлови коишто не се изменети од последната проверка.

П: Колку често треба да правам целосна проверка на мојот компјутер?
О: Под услов да нема пропусти во безбедноста на вашиот систем, заштитата во реално време која што ја обезбедува Kaspersky Internet Security треба да ја елиминира потребата од периодични проверки.

П: Кога правам целосна проверка на мојот компјутер, перформансите на компјутерот се влошуваат значително. Дали можам да направам нешто во врска со тоа?
О: Правењето длабинска проверка на вашиот систем претставува интензивна активност бидејќи има многу тестови што треба да се спроведат на целиот фајл систем. Kaspersky Lab има конкретни технологии како што е iSwift коишто се користат за балансирање на обемот на работа на вашиот систем за време на проверките. Меѓутоа, ние сепак би препорачале да правите целосни проверки во текот на ноќта кога системот не е во функција.

П: Дали можам да видам кои KAV или KIS задачи и процеси се активни во моментот на мојот компјутер?
О: Имате опција секогаш да можете да гледате кои задачи на проверка се извршуваат од страна на софтверот во секое време. KAV/KIS вклучува функција Task Manager (Управувач со задачи) којашто е идеална за најефикасно искористување на ресурсите од вашиот компјутер.

KASPERSKY GADGET

П: Што е Kaspersky Gadget и какви придобивки можам да имам од неговото користење?
О: Kaspersky Gadget е дел од интерфејсот и е лоциран на Windows Desktop. Тој нуди пристап до главните функционалности на софтверот. Ова значи дека корисниците може да стартуваат вообичаени задачи многу брзо. Корисниците можат да дефинираат кои функционалности на софтверот можат да се стартуваат со помош на Kaspersky Gadget. Kaspersky Gadget го прикажува статусот на заштита на компјутерот и ги прикажува KIS/KAV процесите коишто се во тек на компјутерот, како што е проверка и ажурирање на базите на податоци.

П: Дали треба да направам нешто посебно за да го користам Kaspersky Gadget?
О: Не. Kaspersky Gadget ќе се инсталира автоматски на Windows Vista, Windows 7 и Windows 8.

П: Дали можам да го прилагодам изгледот на Kaspersky Gadget?
О: Достапни се два формати: стандарден и максимизиран со проширени функции.

ПЕРФОРМАНСИ И АЖУРИРАЊЕ НА СОФТВЕРОТ

П: Не сакам постојано ажурирање на потписите за злонамерен софтвер на мојот компјутер. Како да го избегнам ова?
О: Достапни ви се неколку опции. Можете да закажете ажурирање коешто ќе се изврши во текот на ноќта или друг пат кога нема да го користите компјутерот, или можете да изберете да правите ажурирање рачно. Доколку само што сте го вклучиле компјутерот, а доцните со ажурирањето, можете да ги подесите KIS и KAV да почекаат претходно дефиниран број на минути пред да започне ажурирањето по вклучувањето.

П: Како да спречам KIS и KAV автоматски да се ажурираат самите?
О: Автоматското ажурирање на софтверот е екстремно корисна алатка која што ви потврдува дека ја имате најнапредната и најефикасната можна заштита. Меѓутоа, ова е опционално и можете да ја исклучите оваа функционалност ако сакате.

П: Колку често ќе добивам ажурирање на софтверот?
О: Ќе добивате ажурирање на софтверот кога тоа е потребно. На пример, кога ќе се појават периодично нови видови на вируси коишто го револуционизираат начинот на којшто вирусите го напаѓаат компјутерот. Затоа Kaspersky Lab ја ажурира софтверската архитектура со цел да се спречи голем удар на перформансите на компјутерот.

П: Како да се забрза процесот на ажурирање?
О: KAV/KIS има пренесено делови од своите антивирусни бази на податоци во “cloud“ и има додадено дополнителна интерна оптимизација. Ова помага значително да се намали обемот на преземен сообраќај и го забрзува процесот на ажурирање.

П: Дали можам да направам лаптопот да ми работи подолго?
О: KAV/KIS го намалува користењето на батеријата со одложување на задачите кои што бараат повеќе ресурси, при што го продолжува животниот век на батеријата на вашиот лаптоп.

КОМПАТИБИЛНОСТ СО ИНТЕРНЕТ ПРЕБАРУВАЧОТ

П: Кои пребарувачи се компатибилни со KAV и KIS ?
О: Палета функционалности и модули на KAV/KIS (URL Advisor, Anti-Banner, Virtual Keyboard, Safe Money, и др.) ги поддржуваат најновите верзии на следниве веб пребарувачи:

- Internet Explorer 8 - 11
- Mozilla Firefox 9.x – 26.x
- Google Chrome 15.x - 27.x
- Opera 12.61

Во овие верзии на пребарувачите, софтверот ги инсталира дополнителните компоненти за брзо повикување на функционалностите на KAV/KIS .

КОМПАТИБИЛНОСТ СО NETBOOK

П: Дали KIS и KAV функционираат на мојот netbook?
О: KIS и KAV се целосно компатибилни со netbook. Тие ги поддржуваат главните резолуции на екранот што се користат на netbook (1024 x 600 и 1366 x 768) и имаат минимално влијание на перформансите.

ФУНКЦИОНАЛНА СПОРЕДБА НА KAV И KIS

Ред. Бр.	Име на компонента/функционалност	KAV	KIS
	Основна заштита		
1	File Anti-Virus	V	V
2	Mail Anti-Virus	V	V
3	IM Anti-Virus	V	V
4	Web Anti-Virus	V	V
5	Smart updates	V	V
	Напредна заштита		
6	Контрола на апликации	-	V
7	Application Activity Control	-	V
8	Услуги базирани на Cloud (репутација)	V	V
9	File Advisor	V	V
10	Automatic Exploit Prevention (Автоматско спречување на експлоатација)	V	V
11	Следач на системот (System Watcher)	V	V
12	Поништување на злонамерни промени	V	V
	Интернет и мрежна безбедност		
13	Safe Money	-	V
14	URL Advisor	V	V
15	Safe Surf	V	V
16	Geo Filter	-	V
17	Firewall	-	V
18	Блокатор на мрежни напади	-	V
19	Network monitor	-	V
	Заштита на дигиталниот идентитет		
20	Anti-Phishing	V	V
21	Виртуелна тастатура	V	V
22	Брзо стартување на Виртуелна тастатура	-	V
23	Безбедносна тастатура	-	V
24	Избришете го историјатот на вашите активности	V	V
25	Контролирајте го пристапот до вашите приватни податоци	-	V
	Блокирање на несакана содржина		
26	Anti-Spam	-	V
27	Anti-Banner	-	V
	Семејна заштита		
28	Напредна родителска контрола	-	V
29	Контрола на користењето на компјутерот и на апликациите	-	V
30	Контрола на комуникациите преку електронска пошта, апликации за испраќање брзи пораки и социјални мрежи	-	V
	Системска безбедност		
31	Диск за спасување на податоците	V	V
32	Проверка на системот по заразувањето со вирус	V	V
33	Security Analyzer	V	V
34	Конфигурација на пребарувачот	V	V
35	Откривање на Rootkit	V	V
	Користење		
36	Подобрување на GUI	V	V
37	Web Installer	V	V
38	Gamer Mode	V	V

СИСТЕМСКИ БАРАЊА ЗА KASPERSKY INTERNET SECURITY

1. За следниве оперативни системи* (некои функционалности на производите можат да работат само на x32 оперативни системи)
- Microsoft Windows XP Home Edition (Service Pack 2 или понова верзија)
- Microsoft Windows XP Professional (Service Pack 2 или понова верзија)
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 или понова верзија)

Хардверски барања
- Процесор: Intel Pentium 1 GHz 32-bit (x86)/64-bit (x64) или повеќе
- 512 MB достапна RAM меморија

2. За следниве оперативни системи* (некои функционалности на производите можат да работат само на x32 оперативни системи)
- Microsoft Windows Vista Home Basic (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Home Premium (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Business (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Enterprise (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Ultimate (32/64 Bit) (Service Pack 1)
- Microsoft Windows 7 Starter
- Microsoft Windows 7 Home Basic (32/64 Bit)
- Microsoft Windows 7 Home Premium (32/64 Bit)
- Microsoft Windows 7 Professional (32/64 Bit)
- Microsoft Windows 7 Ultimate (32/64 Bit)

Хардверски барања
- Процесор: 1 GHz или повеќе
- 1 GB достапна RAM меморија (32 Bit) или 2 GB достапна RAM меморија (64 Bit)

За сите типови на оперативни системи потребно е:
- Приближно 480 MB слободен простор на хард дискот (во зависност од големината на антивирусните бази на податоци)
- Компјутерско глувче
- Интернет конекција – за активирање на софтверот
- Microsoft Internet Explorer 8 или понова верзија
- Microsoft Windows Installer 3.0 или понова верзија
- Microsoft .Net Framework 4

Хардверски барања за Netbook
- CPU: Intel Atom 1.6 GHz
- RAM: 1 GB DDR2
- Хард диск: 160 GB
- Видео картичка: Intel GMA950
- Екран: 10.1 инчи, 1024x600 широк екран
- Оперативен систем: Microsoft Windows XP Home Edition

СИСТЕМСКИ БАРАЊА ЗА KASPERSKY ANTI-VIRUS

1. За следниве оперативни системи* (некои функционалности на производите можат да работат само на x32 оперативни системи)
- Microsoft Windows XP Home Edition (Service Pack 2 или понова верзија)
- Microsoft Windows XP Professional (Service Pack 2 или понова верзија)
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 или понова верзија)

Хардверски барања
- Процесор: Intel Pentium 1 GHz 32-bit (x86)/64-bit (x64) или повеќе
- 512 MB достапна RAM меморија

2. За следниве оперативни системи* (некои функционалности на производите можат да работат само на x32 оперативни системи)
- Microsoft Windows Vista Home Basic (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Home Premium (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Business (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Enterprise (32/64 Bit) (Service Pack 1)
- Microsoft Windows Vista Ultimate (32/64 Bit) (Service Pack 1)
- Microsoft Windows 7 Starter

- Microsoft Windows 7 Home Basic (32/64 Bit)
- Microsoft Windows 7 Home Premium (32/64 Bit)
- Microsoft Windows 7 Professional (32/64 Bit)
- Microsoft Windows 7 Ultimate (32/64 Bit)

Хардверски барања
- Процесор: 1 GHz или повеќе
- 1 GB достапна RAM меморија (32 Bit) или 2 GB достапна RAM меморија (64 Bit)

За сите типови на оперативни системи потребно е:
- Приближно 480 MB слободен простор на хард дискот (во зависност од големината на антивирусните бази на податоци)
- Компјутерско глувче
- Интернет конекција – за активирање на софтверот
- Microsoft Internet Explorer 8 или понова верзија
- Microsoft Windows Installer 3.0 или понова верзија
- Microsoft .Net Framework 4

Хардверски барања за Netbook
- CPU: Intel Atom 1.6 GHz
- RAM: 1 GB DDR2
- Хард диск: 160 GB
- Видео картичка: Intel GMA950
- Екран: 10.1 инчи, 1024x600 широк екран
- Оперативен систем: Microsoft Windows XP Home Edition

СПОДЕЛИ ДОЖИВУВАЊА