

# KASPERSKY LAB

---

**SECURE  
YOUR  
CYBERSPACE**

[www.kaspersky.com](http://www.kaspersky.com)



---

**Kaspersky Anti-Virus® Personal 5.0**

**BRUKERVEILEDNING**

KASPERSKY ANTI-VIRUS® PERSONAL 5.0

---

# Brukerveiledning

© Kaspersky Lab  
<http://www.kaspersky.com>  
<http://www.kaspersky.no>

Revisjonsdato: Oktober 2004

# Innhold

KAPITTEL 1. INTRODUKSJON.....	5
1.1. Datavirus og skadelige programmer.....	5
1.2. Hovedfunksjoner i Kaspersky Anti-Virus Personal.....	6
1.5. Hva er nytt i versjon 5.0?.....	8
1.6. Maskinvare og programvarekrav.....	9
1.7. Programpakken.....	9
1.8. Tjenester for registrerte brukere.....	10
KAPITTEL 2. INSTALLASJON AV PROGRAMMET.....	11
KAPITTEL 3. DERSOM DIN DATAMASKIN ER INFISERT.....	15
3.1. Infeksjonssymptomer.....	15
3.2. Hva skal du gjøre dersom du merker symptomer på infeksjon.....	16
KAPITTEL 4. ANTI-VIRUSBESKYTTELSE VED HJELP AV KASPERSKY ANTI-VIRUS PERSONAL STANDARDINNSTILLINGER.....	18
4.1. Sanntidssøk.....	18
4.2. Skanning.....	19
4.3. Oppdatering av anti-virusdatabasen.....	20
KAPITTEL 5. GRENSESNIITT.....	22
5.1. Oppgave-ikonet.....	22
5.2. Hurtigmeny.....	22
5.3. Hovedvinduet - generell struktur.....	24
5.3.1. <i>Beskyttelse</i> arkfanen.....	25
5.3.2. <i>Innstillinger</i> arkfanen.....	27
5.3.3. <i>Brukerstøtte</i> arkfanen.....	28
5.4. Skannevinduet.....	29
5.5. Applikasjonens referansesystem.....	30
KAPITTEL 6. FOREBYGGING AV VIRUSINFEKSJON.....	31
6.1. Når trenger jeg å kjøre en viruskann?.....	32
6.2. Søkeinnstillinger i bruk.....	33
6.3. Starte en full skann.....	38
6.4. Regelmessig skanning.....	39

6.5. Velg objekter som skal skannes .....	40
6.6. Skanning i arkiver .....	43
KAPITTEL 7. SKANNE EN CD ELLER EN DISKETT .....	46
KAPITTEL 8. INNSTILLING AV SANNTIDSSØK .....	48
8.1. Sjekke beskyttelsesstatusen .....	48
8.2. Spesifisering av handlinger og innstilling av beskyttelsesnivå .....	49
KAPITTEL 9. BESKYTTE E-POST MOT VIRUS .....	54
KAPITTEL 10. BEHANDLING AV INFISERTE OG MISSTENKELIGE OBJEKTER .....	56
KAPITTEL 11. FORNYELSE AV LISENS .....	58
KAPITTEL 12. NEDLASTING AV OPPDATERINGER .....	60
12.1. Når bør du laste ned oppdateringer .....	60
12.2. Laste ned oppdateringer via Internett .....	61
12.3. Laste oppdateringer fra en lokal mappe .....	62
12.4. Oppdatere Kaspersky Anti-Virus Personal applikasjonsmoduler .....	64
12.5. Automatiske oppdateringer .....	64
12.6. Oppdateringer .....	64
KAPITTEL 13. UTVIDEDE INNSTILLINGER .....	66
13.1. Avanserte alternativer for sanntidssøk .....	66
13.2. Avanserte alternativer for skanning .....	69
13.3. Behandle objekter i karantene .....	70
13.4. Innstillinger for karantene .....	72
13.5. Behandle rapporter .....	73
13.5.1. Se informasjon i rapporter .....	77
13.5.2. Eksportere og sende rapporter .....	78
13.6. Utvidede innstillinger .....	79
VEDLEGG A. KONTAKTE BRUKERSTØTTE .....	81
VEDLEGG B. ORDLISTE .....	83
VEDLEGG C. KASPERSKY LAB .....	88
C.1. Andre Kaspersky Lab produkter .....	89
C.2. Kontaktinformasjon .....	92
VEDLEGG D. LISENSAVTALE .....	94

---

# KAPITTEL 1. INTRODUKSJON

## 1.1. Datavirus og skadelige programmer

Når antallet databrukere øker - og datautveksling via Internett og e-post stadig blir mer tilgjengelig, merker man en stadig økende trussel for virusinfeksjoner og dataødeleggelse, eller innsamling av data av skadelige eller ondsinnede programmer (malware)

For at du skal være oppmerksom på disse potensielle truslene, er det nyttig å vite hvilke typer skadelig programvare ("malware") som finnes, og hvordan de fungerer. Generelt kan vi si at skadelige programmer finnes i tre kategorier:

- **Ormer** ("Worms") benytter nettverksressuser for distribusjon. Disse programmene blir kalt ormer forde de kan gå gjennom tunneler fra en datamaskin til en annen - ved hjelp av nettverk, e-post eller andre kanaler. Ormer kan spre seg ekstremt raskt.

Ormer penetrerer en datamaskin, fastslår IP-adresser til andre datamaskiner og sender kopier av seg selv til disse datamaskinene. Ormer kan også benytte seg av data i adressebøker lagret i e-postprogrammet på den infiserte maskinen. Ormer kan også lage arbeidsfiler på lokale lagringsmedier - men kan ikke benytte seg av andre ressurser enn minnet på den infiserte datamaskinen.

- **Virus** ("Viruses") infiserer dataprogrammer ved å endre måten programmet fungerer for å ta kontroll når det infiserte programmet kjører. Denne enkle definisjonen hjelper til å fastslå at hovedmetoden et virus fungerer på er ved å infiserer dataprogrammer. Virus sprer seg i hovedsak litt saktere enn ormer.
- **Trojanske hester** ("Trojan horses") utøver uautoriserte handlinger på infiserte datamaskiner. For eksempel kan de: slette informasjon på lokale lagringsmedier, "fryse" systemet eller stjele konfidensiell informasjon. Dersom vi ser snevert på det, kan vi sis at trojanske hester ikke er virus - siden de ikke infiserer dataprogrammer eller data, og at de ikke kan komme seg inn "selvstendig" på datamaskin - men sprer seg gjennom "hjelpesprogrammer" laget av ondsinnede brukere. Uansett: skade som kan oppstå fra en trojan er mye større en skade fra et vanlig virusangrep.

I det siste er ormer den mest utbredte (eller vanlige) typen skadelig kode, deretter følger virus og så trojaner. Noen skadelige programmer benytter seg av flere funksjoner fra de tre kategoriene - og noen også av alle kategoriene.

Selv om skadelige programmer i hovedsak distribueres via e-post og Internett, kan disketter eller CD-er også være kilder til infeksjoner. Derfor er nå oppgaven med å beskytte mot potensielle trusler nå mye mer enn enkle virusskanninger. Den inkluderer også den komplekse oppgaven med effektiv sanntidsbeskyttelse.



Derfor vil denne hjelpefilen ved å benytte terminologien "virus" henvise til alle tre kategorier nevnt her: virus, ormer og trojaner. Spesielle former for skadelig koder vil bli beskrevet dersom dette er nødvendig.

## 1.2. Hovedfunksjoner i Kaspersky Anti-Virus Personal

Kaspersky Anti-Virus® Personal (heretter kalt Kaspersky Anti-Virus eller applikasjonen) er utviklet for yte anti-virusbeskyttelse på frittstående datamaskiner som benytter Microsoft Windows operativsystem (se avsnittet Maskinvare og programvarekrav).

Kaspersky Anti-Virus® utfører følgende funksjoner:

- **Beskyttelse mot virus og skadelige dataprogram** - applikasjonen oppdager og utrydder virus som forsøker å penetrere datamaskin via flytbare eller stasjonære lagringsmedier, e-post eller Internett. Når applikasjonen brukes, kan følgende modi brukes (enten samlet eller hver for seg):
  - **Sanntids anti-virus** - utfører anti-viruskanning av alle objekter som kjøres, åpnes eller lagres.
  - **Skanning** - utfører anti-viruskanning og desinfisering av hele din datamaskin eller valgte mapper, stasjoner eller filer. Skanning kan startes enten manuelt eller ved regelmessige intervaller.
- **Gjenopprettelse etter virusangrep** - ved å kjøre full skann og rens, med innstillinger anbefalt av Kaspersky Lab, vil du utrydde alle virus som har infisert din datamaskin under et virusangrep.
- **Skanning og rensing av innkommende/utgående e-posttrafikk** - sanntidssøk utfører konstant anti-viruskanning og rensing av innkommende e-postmeldinger før de lastes ned til din innboks<sup>1</sup>, og av

---

<sup>1</sup> Programmet sjekker kun e-postmeldinger som mottas via POP3 protokollen eller sendes via SMTP protokollen.

utgående e-post. I tillegg skanner og renser programmet e-postdatabasene til forskjellige e-postklienter<sup>2</sup> (se også avsnittet Beskyttelse av e-post mot virus).

- **Oppdatering av anti-virusdatabasen og applikasjonsmoduler** - beskyttelsen av din datamaskin holdes oppdatert ved hjelp av automatiske funksjoner som oppdaterer anti-virusdatabasen med informasjon om nye virus, og nye metoder for å rense objekter som infiseres av disse virusene. Oppdateringer lastes ned fra Kaspersky Labs oppdateringsservere, og lagres lokalt på din datamaskin.
- **Anbefalinger om programinnstillinger og handlinger** - tips fra Kaspersky Lab hjelper deg mens du bruker Kaspersky Anti-Virus. Installasjonen er raskere og enklere fordi standardinnstillinger er anbefalte innstillinger for optimal anti-virusbeskyttelse.

Når infiserte eller mulig infiserte filer oppdages, anti-virusdatabasen ikke er oppdatert på lenge, eller din datamaskin ikke er skannet på lenge - vil hovedvinduet i Kaspersky Anti-Virus anbefale en handling, med utfyllende informasjon. Vi har tilpasset applikasjonen for å oppnå optimal ytelse basert på den omfattende ekspertisen Kaspersky Lab har innenfor anti-virusbeskyttelse, og på tilbakemeldinger fra våre brukere. Anbefalt beskyttelseinnstillinger blir installert som standardinnstillinger i programmet.

- **Karantene** - en sikker lagringsplass hvor mulig infiserte objekter oppbevares. Du kan rense eller slette objekter i karantene, gjenopprette til sin originale plassering eller sende de til Kaspersky Lab for analyse. Karantenefiler lagres i et spesielt format, og utgjør ingen trussel for din datamaskin.
- **Rapporter** - resultat fra alle handlinger utført av Kaspersky Anti-Virus dokumenteres i rapportene. En detaljert skannerapport inneholdende statistikker over alle skannede objekter, innstillinger brukt for oppgavene og historikk over handlinger utført på hver fil. Rapporter genereres også under sanntidssøk og etter oppdatering av anti-virusdatabasen og applikasjonsmodulene.

---

<sup>2</sup> Kaspersky Anti-Virus kan skanne e-postdatabase for alle e-postprogrammer, men kan kun rense MS Outlook og MS Outlook Express e-postdatabaser.

## 1.3. Hva er nytt i versjon 5.0?

Kaspersky Anti-Virus Personal 5.0 har følgende funksjoner som ikke finnes i versjon 4.5:

- *Vedlikehold av database for skannede objekter.* Versjon 5.0 skanner ikke tidligere analyserte objekter som ikke er endret siden siste skanning. Dette gjelder både sanntidssøk og full skanning. Denne funksjonen gjør at hastighet og ytelse for programmet økes kraftig.
- Versjon 5.0 *beskytter e-post mot virus* uansett hvilken klient som mottar e-post via POP3 protokollen, eller sender via SMTP protokollen. Tidligere versjoner beskyttet kun Microsoft Exchange-kompatible e-postklienter.
- *Rensing i arkiver.* Versjon 5.0 renser infiserte filer i zip, arj, cab, og rar arkiver. Tidligere versjon kunne kun rense i zip-arkiv.



Kaspersky Anti-Virus skanner selvutpakkende arkiver, men kan ikke rense disse.

- *Brukervennlig grensesnitt.* Versjon 5.0 er nå kun en applikasjon - mot tidligere versjoner som bestod av flere komponenter som hver utførte bestemte anti-virus funksjoner. Denne nye retningen forenkler kontroll over de viktigste programfunksjonene. For eksempel kan beskyttelsesnivået enkelt endres ved å flytte på en rullemeny - fremfor å redigere de enkelte alternativene.
- *Anbefalte innstillinger og ekspertråd.* For å ytterligere forenkle programmets oppgaver er nå standardinnstillinger anbefalt av Kaspersky Labs, slik at det ikke lenger er behov for å konfigurere programmet før bruk. Når anti-virusbeskyttelsen er satt til **Høy hastighet** vises i tillegg et varsel som anbefaler et høyere beskyttelsesnivå.
- *Fornyelse av lisens.* Nytt i versjon 5.0 er installasjon av ny lisensnøkkel og fornyelse av lisensperioden.
- *Sende filer til analyse hos Kaspersky Lab.* Nå kan du sende oss mulig infiserte filer som oppdages av versjon 5.0 - eller filer du misstenker er infisert - til analyse.
- *Muligheter for å slette infiserte sammensatte objekter er fjernet.* Det er ikke lenger mulig å slette infiserte sammensatte objekter (arkiver, e-postdatabase eller e-postmeldinger) i versjon 5.0. Det er mulig å slette slike objekter (med unntak av selvutpakkende arkiver) ved hjelp av standard Windows-verktøy - som Windows Utforsker.

## 1.4. Maskinvare og programvarekrav

For normal ytelse av Kaspersky Anti-Virus Personal 5.0, må din datamaskin møte følgende minimumskrav:

Genrelle krav:

- 50 MB tilgjengelig lagringsplass på lokal stasjon
- CD-ROM stasjon (for installasjon av Kaspersky Anti-Virus fra CD)
- Microsoft Internet Explorer 5.5 (for oppdatering av anti-virusdatabasen og applikasjonsmoduler over Internett)

Windows 98:

- Intel Pentium 133 MHz prosessor
- 32 MB RAM

Windows ME:

- Intel Pentium 150 MHz prosessor
- 32 MB RAM

Windows NT Workstation 4.0 (Servicepakke 6a):

- Intel Pentium 133 MHz prosessor
- 32 MB RAM

Windows 2000 Professional (Servicepakke 2 eller nyere):

- Intel Pentium 133 MHz prosessor
- 64 MB RAM

Windows XP Home Edition eller XP Professional (Servicepakke 1 eller nyere):

- Intel Pentium 300 MHz prosessor
- 128 MB RAM

## 1.5. Programpakken

Du kan bestille våre produkteter (online eller eske) via våre forhandlere eller gjennom våre nettsider (<http://www.kaspersky.no>, og gå til nettbutikk).

Innholdet i esken inneholder følgende:

- 1 stk forseglet CD eller disketter med programvaren.

- Brukermanualen.
- Lisensnøkkelen på en diskett.
- Lisensavtalen.



Før du bryter forseglelsen på CD (eller diskettene), les nøye igjennom Lisensavtalen som følger med.

Dersom du bestiller Kaspersky Anti-Virus® online, kan du laste ned programmet og brukermanualen direkte fra våre nettsider (<http://www.kaspersky.no>). Lisensnøkkelen vil bli sendt til deg via e-post.

Lisensavtalen er en gyldig kontrakt mellom deg og Kaspersky lab som beskriver betingelsene og vilkårene for bruken av produktet du har kjøpt.

Vennligst les nøye igjennom Lisensavtalen.

Dersom du ikke godtar med betingelsen og vilkårene i Lisensavtalen, vennligst returner esken til den forhandleren du har kjøpt produktet fra. Du vil få refundert beløpet bare dersom forseglelsen på CD (og diskettene) ikke er brutt.

Ved å bryte forseglelsen på CD (og diskettene), godtar du betingelsene og vilkårene som beskrevet i Lisensavtalen.

## 1.6. Tjenester for registrerte brukere

Kaspersky Lab tilbyr alle registrerte brukere omfattende tjenesteytelser som gjør det mulig å bruke Kaspersky Anti-Virus mer effektivt.

Etter kjøp av lisens blir du automatisk en registrert bruker - og i din lisensperiode kan vi tilby følgende tjenester:

- Oppdatering av anti-virusdatabasen og applikasjonsmoduler
- brukerstøtte for spørsmål relatert til installasjon, konfigurasjon og bruk av programmet. Brukerstøtte tilbys per telefon eller e-post
- informasjon om Kaspersky Lab produkter. Du kan også abonnere på nyhetsbrev som inneholder informasjon om nye datavirus etter hvert som de oppdages.



Kaspersky Lab yter ikke brukerstøtte for spørsmål relatert til ytelse av operativsystemer eller andre teknologier.

---

# KAPITTEL 2. INSTALLASJON AV PROGRAMMET

For å installere Kaspersky Anti-Virus på din datamaskin, må du kjøre filen **kavsetup.exe** fra installasjonsmappen/CD.

Installasjonsveilederen jobber interaktivt - og hver dialogboks har følgende knapper du kan bruke i installasjonsprosessen:

- **Neste>** - godkjenne og fortsette med installasjonen.
- **<Tilbake** - tilbake til forrige dialogboks i installasjonsprosessen
- **Avbryt** - avbryter installasjonen
- **Fullfør** - avslutter installasjonen

En detaljert beskrivelse av hvert ledd i installasjonsprosessen følger under.

## Steg 1. Sjekk av hvilket operativsystem som er installert på din datamaskin.

Før installasjonen starter, sjekkes ditt operativsystem og Servicepakker for å påse at de oppfyller minimumskravene for installasjon av Kaspersky Anti-Virus.

Dersom programmet finner ut at noen av de påkrevde Servicepakkene ikke er installert, vil du bli varslet om at du må installere disse ved hjelp av **Windows Update** før du kan fortsette med installasjonen av Kaspersky Anti-Virus.

## Steg 2. Søk etter andre anti-virusprogrammer.



**Dette leddet er kun nødvendig dersom det oppdages andre anti-virusprogram på din datamaskin**

Neste steg involverer søk etter andre installerte anti-virusprogram (inkludert andre Kaspersky Lab programmer). Dette utføres fordi samtidig bruk av slike programmer med Kaspersky Anti-Virus kan medføre konflikter.

Dersom en tidligere versjon av Kaspersky Anti-Virus blir oppdaget, vil du bli varslet om å avinstallere dette.



Vi anbefaler at før du fjerner tidligere versjoner av programmet (Kaspersky Anti-Virus Personal/Personal Pro 4.x) lagrer lisensnøkkelen programmet bruker. Denne nøkkelen kan også brukes for Kaspersky Anti-Virus Personal 5.0

klikk OK og avinstaller tidligere versjoner av Kaspersky Anti-Virus, kjør deretter kavsetup.exe på nytt.

Dersom anti-virusprogram fra en annen produsent blir oppdaget på din datamaskin, vil du bli varslet om å avinstallere dette programmet før du fortsetter installasjonen av Kaspersky Anti-Virus.

Vi anbefaler at du avbryter installasjonen av Kaspersky Anti-Virus og avinstallerer det (de) andre programmet/programmene. For å gjøre dette, klikk **Nei**, avinstaller programmet/programmene, og kjør deretter kavsetup.exe på nytt.

Dersom det oppdages at Kaspersky Anti-Virus Personal 5.0 allerede er installert på din datamaskin, vil du bli varslet om dette - men en advarsel om at dersom du fortsetter med denne installasjonen vil eksisterende installasjon blir overskrevet med den nye installasjonen.

### Steg 3. Starte installasjonsveilederen

Dersom ikke andre anti-virusprogrammer blir oppdaget, vil du se en dialogboks som bekrefter at Kaspersky Anti-Virus installasjonsveileder har begynt.

For å fortsette installasjonen, klikk **Neste>**. For å avbryte installasjonen, klikk **Avbryt**

### Steg 4. Les lisensavtalen

Neste dialogboks inneholder lisensavtalen mellom deg og Kaspersky Lab på engelsk. Les den nøye og klikk **Godta** dersom du godtar alle vilkårene i avtale. Installasjonsprosessen vil da fortsette.

### Steg 5. Brukerinformasjon

Neste dialogboks ber om brukernavn og navn på firma. Standardinformasjon kopieres fra operativsystemets register, og du kan endre informasjonen om du ønsker.

For å fortsette installasjonen, klikk **Neste>**.

## Steg 6. Les viktig informasjon om programmet

Vi anbefaler at du leser nøye gjennom viktig informasjon om programmet før du begynner å bruke det.

Denne dialogboksen inneholder informasjon om hovedfunksjoner og kjennetegn i Kaspersky Anti-Virus.

Etter du har lest informasjonen, klikk **Neste >**.

## Steg 7. Installere lisensnøkkel



Dette utføres kun dersom Kaspersky Anti-Virus installasjonsveileder ikke finner nøkkelen automatisk

I dette steget installeres lisensnøkkel for Kaspersky Anti-Virus. Lisensnøkkelen er din personlige "nøkkel" som inneholder all nødvendig tjenesteinformasjon som er påkrev for komplett drift av Kaspersky Anti-Virus Personal:

- Teknisk brukerstøtteinformasjon (leverandør av brukerstøtte og kontaktinformasjon).
- Lisensnavn, nummer og utløpsdato.



Programmet virker ikke uten lisensnøkkel.

Finn lisensnøkkelen ved hjelp av standard filvalgsdialog og klikk Neste > for å fortsette installasjonen.

Dersom du ikke har lisensnøkkel når du installerer programmet, kan du installere nøkkelen senere - når programmet startet opp første gang. Husk du ikke kan bruke Kaspersky Anti-Virus uten lisensnøkkel.

## Steg 8. Velg installasjonsmappe

Nå kan du velge målmappe for programfilene. Standard sti er: **C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus Personal.**

For å endre stien klikk **Bla gjennom...**, og spesifiser ny installasjonsmappe og klikk **Neste >**.

Da vil Kaspersky Anti-Virus applikasjonsfiler bli kopiert til din datamaskin.

## Steg 9. Avslutt installasjonen

Nå vil dialogboksen **Avslutter installasjonsveiviser** informere deg om at installasjonen av Kaspersky Anti-Virus til din datamaskin er fullført.

Dersom registrering av systemtjenester er påkrevd, vil du bli bedt om å starte din datamaskin på nytt. Dette er et PÅKREVD sted for å fullføre installasjonen av programmet.



*For å fullføre installasjonen:*

1. Velg et av følgende alternativer
  - Ja, jeg vil starte min datamaskin på nytt nå**
  - Nei, jeg vil starte min datamaskin på nytt senere**
2. Klikk **Ferdig**



*Dersom din datamaskin ikke trenger omstart for å fullføre installasjonen, kan du begynne å bruke programmet med en gang. Utfør følgende steg for å fullføre installasjonen:*

1. Dersom du ikke ønsker å starte beskyttelsen av din datamaskin etter installasjonen er fullført, avmarker alternativet **Kjør Kaspersky Anti-Virus Personal 5.0**.



Dersom du fjerner markeringen av dette alternativet, vil beskyttelsen av din datamaskin automatisk starte ved neste oppstart etter omstart. Før dette kan du starte programmet fra Windows Startmeny (**Start → Programmer → Kaspersky Anti-Virus Personal**).

2. Klikk **Ferdig**.

---

# KAPITTEL 3. DERSOM DIN DATAMASKIN ER INFISERT...

Noen ganger er det ikke åpenbart, selv for velinformerte brukere, at en datamaskin er infisert med virus - fordi virus effektivt kamuflerer seg blant vanlige filer. Dette kapitlet inneholder detaljert beskrivelse av infeksjonssymptomer, metoder for gjenoppretting av data etter virusangrep og tiltak for forhindring av dataødeleggelse grunnet virus

## 3.1. Infeksjonssymptomer

Det finnes mange symptomer som kan bety at din datamaskin er infisert. Dersom du oppdager "merkelige ting" som skjer med din datamaskin - som for eksempel:

- uventede meldinger eller bilder som plutselig dukker opp
- uvanlige lyder eller musikk som spilles vilkårlig
- CD-ROM skuffen åpner og lukker seg av seg selv
- programmer starter plutselig på din datamaskin
- dersom Kaspersky Anti-Hacker er installert på din datamaskin, vil denne varsle om programmer som forsøker å koble seg til Internett - selv om du ikke har innledet en slik oppgave.

Dersom noen av de nevnte symptomene oppstår, er det svært sannsynlig at din datamaskin er infisert av ett eller flere virus.

I tillegg finnes det typiske symptomer på at din datamaskin er blitt infisert via e-post:

- dine venner nevner at de har mottatt meldinger fra deg - men du har aldri sendt disse meldingene
- din e-postkonto inneholder mange meldinger uten avsenders e-postadresse eller meldingshode

Vær oppmerksom på at disse problemene kan forårsakes av andre årsaker enn datavirus. For eksempel kan meldinger med din adresse som avsender være sendt fra en annen datamaskin.

Det finnes også indirekte symptomer på at din datamaskin muligens er infisert av virus:

- din datamaskin stopper å fungere (henger seg) regelmessig - eller støter på problemer
- din datamaskin yter merkbart dårligere når programmer kjøres
- du kan ikke laste operativsystemet
- filer og mapper forsvinner plutselig - eller innholdet endres
- lokale stasjoner jobber for mye (hurtig blinking av lysindikator)
- Microsoft Internet Explorer "henger seg " eller oppfører seg rart (for eksempel hvis du ikke kan avslutte programmet)

90% av slike indirekte symptomer indikerer at du kan ha ett maskinvare eller programvare problem, men slike symptomer kan også forårsakes av en infeksjon. Vi anbefaler at du starter en full skanning av din datamaskin med standard innstillinger (anbefalt av Kaspersky Labs eksperter) dersom du møter på noen av disse problemene

## 3.2. Hva skal du gjøre dersom du merker symptomer på infeksjon



*Dersom du oppdager at din datamaskin viser "misstenkelig" oppførsel:*

1. Det er ingen grunn til å få panikk. Denne hovedregelen kan forebygge tap av viktige data lagret på din datamaskin - og hjelpe deg å unngå unødvendig stress.
2. Koble din datamaskin fra Internett. Dette er viktig fordi om du er koblet til Internett, kan et virus sende informasjon til inntrengerne eller kan forsøke å spre seg selv ved å benytte e-postadresser i din adressebok
3. Dersom din datamaskin er koblet til et lokalt nettverk, koble fra nettverket.
4. Dersom symptomet på en infeksjon er at du ikke kan starte fra lokale stasjoner (at din datamaskin varsler om problemer under oppstart), forsøk å starte systemet i Sikkerhetsmodus - eller fra Windows oppstartsdisketter som du lagde under installasjon av ditt operativsystem
5. Før du utfører noen handlinger, ta sikkerhetskopi av kritiske data til et flyttbart medie (for eksempel diskett, cd, flashminne, USB-stasjon etc)

6. Installer Kaspersky Anti-Virus dersom du ikke har installert det ennå
7. Last ned de nyeste oppdateringene til anti-virusdatabasen. Dersom det er mulig, benytt en annen datamaskin enn den infiserte til å laste ned oppdateringene. Du kan også motta anti-virusdatabasen på en CD-ROM eller diskett fra Kaspersky Lab eller en autorisert forhandler - og deretter oppdatere din database (for detaljert beskrivelse, se avsnittet Laste ned oppdateringer til en lokal mappe).
8. Aktiver anbefalte innstillinger (se avsnittet Søkeinnstillinger i bruk).
9. Kjør en full skann av systemet (se avsnittet Starte en full skann)


---

# KAPITTEL 4. ANTI-VIRUSBESKYTTELSE VED HJELP AV KASPERSKY ANTI-VIRUS PERSONAL STANDARDINNSTILLINGER

Du kan bruke Kaspersky Anti-Virus umiddelbart etter installasjon. Du trenger ikke definere programmet før du starter å bruke det - siden programmets standardinnstillinger er en optimal balanse mellom ytelse og sikkerhet.

I relaterte emner, beskrives standardinnstillinger i detalj

## 4.1. Sanntidssøk

Umiddelbart etter programmet kjøres (som indikeres av det røde  ikonet på oppgavelinjen), og Kaspersky Anti-Virus skanner alle objekter som kjøres ved oppstart, så vel som *datamaskinens minne og sine egne applikasjonsmoduler*.

Standard sanntidssøk er:

- Objekter som åpnes, lagres eller kjøres på din datamaskin og flyttbare medier som er *potensielt infiserbare* vil skannes, inkludert:
  - *oppstartsektor (disse objektene skannes umiddelbart etter systemoppstart)*
  - *pakkede filer og objekter som er lenket eller innebygd i andre filer (OLE-objekter)*
  - *innkommende e-postmeldinger (når de mottas)*



Sanntidssøk skanner ikke objekter som ikke kan inneholde virus.


- Når ett *infisert objekt* oppdages, blokkerer applikasjonen tilgang til objektet og spør etter handlingsalternativ
- Når ett *mistenkelig eller infisert objekt* oppdages, blokkerer applikasjonen tilgang til objektet og spør etter handlingsalternativ



- Alle handlinger applikasjonen utfører dokumenteres i rapporter (se avsnittet Behandle rapporter).

Sanntids anti-virusbeskyttelse blir automatisk aktivert rett etter systemet starter opp, og er aktivt helt til systemet skrur av.



*Du kan deaktivere sanntidssøk manuelt:*

- Høyreklikk ikonet  på oppgavelinjen.
- Når hurtigmenyen vises, velg **Deaktiver Sanntidssøk**.

Sanntidsbeskyttelsen av din datamaskin skrues da av, og det aktive  ikonet (rødt) blir erstattet med det inaktive  ikonet (grått).



*Vi anbefaler at du ikke deaktiverer sanntidsbeskyttelsen av din datamaskin, da dette dramatisk øker sannsynligheten for en virusinfeksjon.*

## 4.2. Skanning

Ved **Skanning** analyserer programmet hele din datamaskin, eller spesifiserte objekter, stasjoner eller filer. Følgende er standard innstillinger:

En skanning av din datamaskin inkluderer:

- en skann av din datamaskin vil skanne all objektene på dine lokale stasjoner, inkludert:
  - Objekter som kjøres ved oppstart og oppstartsektor
  - arkiver, pakkefile og selvutpakkende arkiv
  - objekt lenket eller innebygd i en annen fil (*OLE-objekt*)
  - datamaskinens Minne som er i bruk
- en skann av en spesifisert disk, mappe eller fil skanner alle objektene i plasseringen, inkludert:
  - *arkiv, pakkefile og selvutpakkede arkiv*
  - objekt lenket eller innebygd i en annen fil (*OLE-objekt*)
- ved oppdagelse av et infisert objekt blir brukeren spurt om handling
- ved oppdagelse av et mistenkelig objekt blir brukeren spurt om handling

- resultatet av skanningen blir dokumentert i rapporter (se seksjon Behandle rapporter).

Som standard er en komplett skann av din datamaskin planlagt å starte automatisk hver Fredag klokken 18:00. Status for skanningen finner du i høyremenyen på **Beskyttelse** arkfanen




### En komplett skann av din datamaskin er startet

Dersom din datamaskin er skrudd av på det oppsatte tidspunktet, vil skanningen ikke bli gjennomført.



*For å starte manuelt en komplett skann av din datamaskin:*

høyre-klikk  systemikonet på oppgavelinjen. I hurtigmenyen, velg **Skann min datamaskin**.

eller

velg **Beskyttelse** arkfanen, og klikk Skann min datamaskin.

## 4.3. Oppdatering av anti-virusdatabasen


Programmet oppdager virus og rensr infiserte objekter ved hjelp av anti-virusdatabasen, som inneholder definisjoner av alle kjente virus, og metoder for rensing.

Det er veldig viktig at anti-virusdatabasen blir regelmessig oppdatert - siden nye virus oppdages daglig.

**Oppdater anti-virusdatabasen** er en veldig viktig funksjon av Kaspersky Anti-Virus. Som standard oppdateres databasen automatisk fra Kaspersky Labs oppdateringsservere og installeres på din datamaskin hver tredje time. Dersom du bruker din datamaskin mindre enn tre timer hver dag, anbefaler vi at du enten endrer oppdateringsintervallet, lar din datamaskin være på eller oppdaterer anti-virusdatabasen manuelt. Gjør du ikke dette, vil ikke anti-virusdatabasen oppdateres.



Du kan oppdatere anti-virusdatabasen manuelt ved å gjøre følgende:

Høyre-klikk  ikonet til høyre på oppgavelinjen. Når hurtigmenyen vises, velg **Oppdater anti-virusdatabasen**.

eller

åpne **Beskyttelse** arkfanen i applikasjonens hovedvindu - og klikk Oppdater nå i venstre menyseksjon.

eller

klikk lenken Oppdater anti-virusdatabasen i høyre menyseksjon av **beskyttelse** arkfanen.



For ytterlige informasjon om oppdatering av anti-virusdatabasen, se avsnittet [Nedlasting av oppdateringer](#).



---



# KAPITTEL 5. GRENSESNIITT

Kaspersky Anti-Virus har et enkelt å lettvindt brukergrensesnitt. I dette emnet forklares hovedelementene i grensesnittet: oppgave-ikonet, hurtigmenyen, hovedvinduet og tjenestevinduene.

## 5.1. Oppgave-ikonet

Når programmet starter, vil et ikon vise beskyttelsesstatus for sanntidssøk på oppgavelinjen ("system tray")

Når sanntidssøk er aktivert, vises ikonet i rødt (aktiv status) ; når sanntidssøk ikke er aktivert, vises ikonet i grått (innaktiv) , selv om e-post og skriptskanning er aktivert.

Når programmet skanner din datamaskin eller stasjoner/filer, og når det analyserer et objekt i sanntid - vil du se at ikonet blinker som en hvit og blå mappe  eller . Når e-post skannes vises en konvolutt istedenfor mappen.


Når en viktig virushendelse oppstår, vil anbefalt handling vises i en varslingsmelding over ikonet



Bilde 1. Varslingsmelding

## 5.2. Hurtigmeny

For å åpne hurtigmenyen, høyreklikk over systemikonet på oppgavelinjen. Menyen inneholder følgende elementer:

- **Åpne Kaspersky Anti-Virus** - åpner hovedvinduet med Beskyttelse arkfanen aktivert. Du kan også åpne hovedvinduet ved å dobbelt-klikke  ikonet på oppgavelinjen.

- **Skann min datamaskin** - utfører en full skann av din datamaskin etter virus med valgte beskyttelsesnivå.
- **Oppdater anti-virusdatabasen** - oppdaterer anti-virusdatabasen fra Kaspersky Labs oppdateringsservere.
- **Deaktiver/Aktiver sanntidssøk** - skru på eller av sanntidsbeskyttelsen av din datamaskin. Programikonets farge beskriver statusen for tjenesten



Vi anbefaler ikke å deaktivere sanntidssøk, da dette dramatisk øker sannsynligheten for virusinfeksjon.

- **Om** - viser generell informasjon om Kaspersky Anti-Virus Personal.
- **Avslutt** - avslutter Kaspersky Anti-Virus og avlaster det fra din datamaskins minne.



Du kan ikke benytte **Avslutt** handlingen i hurtigmenyen om du ikke har administrative rettigheter på datamaskinen.



Bilde 2. Hurtigmeny

## 5.3. Hovedvinduet - generell struktur

Hovedvinduet gir der enkelt tilgang til alle av programmets anti-virusbeskyttelses muligheter. Fra dette vinduet kan du utføre følgende funksjoner:

- konfigurere innstillinger for anti-virusbeskyttelse
- start og stoppe skanning av hele systemet eller spesifiserte stasjoner, mapper eller filer
- laste ned oppdateringer til anti-virusdatabasen og applikasjonsmodulene
- definere tidsintervaller for skanning og oppdateringer
- behandle objekter i karantenen
- behandle rapporter m.v.

Alle innstillingene for anti-virusbeskyttelse, statusinformasjon og de enkelte oppgaver er tilgjengelige fra følgende arkfaner i hovedvinduet:

- **Beskyttelse arkfanen** - oppsummerer nåværende beskyttelsesstatus og gir lett tilgang til skanning. Denne arkfanen er hovedkomponenter i grensesnittet
- **Innstillinger arkfanen** - viser innstillinger og status for alle anti-virusoppgaver
- **Brukerstøtte arkfanen** - viser lisens-, kontakt- og annen brukerstøtteinformasjon

Hver arkfane har to seksjoner:

- *Venstre seksjon* viser en liste med oppgaver som sikrer anti-virusbeskyttelse av din datamaskin. Hver arkfane har sin egen liste med oppgaver:

For eksempel, **Beskyttelse** gir deg en mengde oppgaver relatert til anti-virusskanning. **Innstillinger** arkfanen inkluderer kontroll av parametere for disse oppgavene. **Brukerstøtte** arkfanen gir deg kontroll av oppgaver relatert til brukerstøtte for anti-virusbeskyttelse.

- *Høyre seksjon* inneholder informasjon om nåværende status for anti-virusbeskyttelsen på din datamaskin, inkludert sanntidssøk, skanning, anti-virusdatabasen og lisensinformasjon.

Dermed kan for eksempel **Beskyttelse** arkfanen vise status for nåværende applikasjonsinnstillinger, og **Brukerstøtte** arkfanen viser lisensstatus (lisensnøkkelinformasjon), kontaktinformasjon for brukerstøtte og informasjon om programmet og systemet.

De tre tilstandene av anti-virusbeskyttelse indikeres i **Beskyttelse** og **Innstillinger** arkfanene med følgende ikoner:



*Kritisk tilstand av anti-virusbeskyttelse*

Denne statusen betyr at sanntidssøk er skrudd av eller enkelt oppgaver (skanning og/eller oppdatering) ikke er utført på lenge, eller at nåværende beskyttelsesnivå ikke gir tilstrekkelig anti-virusbeskyttelse av din datamaskin.



*Anti-virusbeskyttelsen er ikke tilsvarende anbefalt nivå*

Dette betyr at nåværende innstillinger for anti-virusbeskyttelsen ikke tilsvarer beskyttelsen i anbefalt nivå eller at et bestemt oppgave må utføres.



*Anti-virusbeskyttelsen er satt til anbefalt nivå*

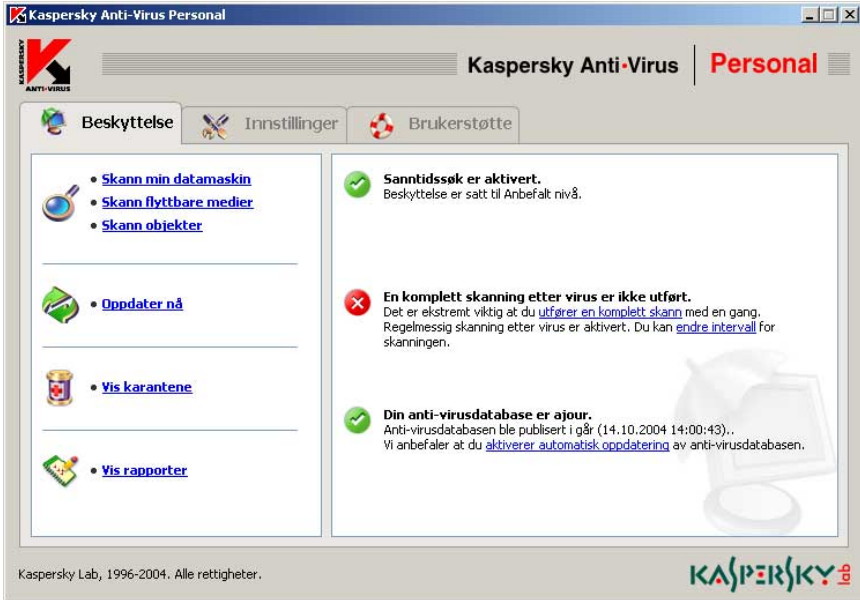
Dette betyr at dine innstillinger tilsvarer innstillinger anbefalt av Kaspersky Lab.

Statusinformasjonen i vises i følgende rekkefølge: først sanntidssøk, så skanning deretter gyldigheten av anti-virusdatabase.

Hver tilstand beskrevet ovenfor kommer med kommentarer og anbefalinger. Dermed vil, for eksempel hvis nåværende beskyttelsesnivå ikke tilsvarer anbefalt nivå - vil du bli varslet om å gjenopprette anbefalte innstillinger for å sikre en optimal beskyttelse.

### **5.3.1. Beskyttelse** arkfanen

Ved å bruke **Beskyttelse** arkfanen, kan du skanne hele din datamaskin eller individuelle stasjoner, mapper eller filer. Du kan også: oppdatere anti-virusdatabasen, se fremdriftsrapporter for alle oppgaver som kjøres, og behandle objekter i karantene. Oppgavene kan startes ved å klikke lenken for oppgaven i venstre menyseksjon.



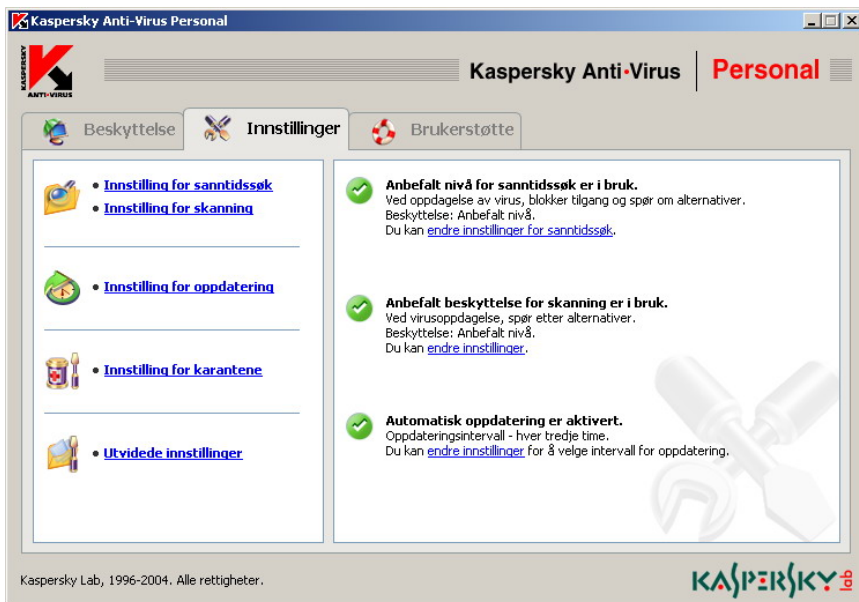
Bilde 3. Beskyttelses arkfanen

I høyre menyseksjon kan du se *nåværende status for sanntidssøk, skanning og anti-virusdatabasen*. I bildet over vises at sanntidssøk er aktivert, men at en full skann ikke er gjennomført. Du kan også se kommentarer for hver av oppgavene

Dersom beskyttelsesstatusen ikke tilsvarer anbefalt nivå, vil du varsles om dette - og spurt om du ønsker å endre innstillingene, gjenopprette anbefalt nivå eller starte en bestemt oppgave. Alle spørsmål eller anbefalinger vises som klikkbare lenker, slik at du lettvis kan utføre ønsket handling.

## 5.3.2. Innstillinger arkfanen

Ved å bruke **Innstillinger** arkfanen kan du evaluere og tilpasse både standard og avanserte innstillinger for å sikre en bra ytelse av Kaspersky Anti-Virus.



Bilde 4. Innstillinger arkfanen

Høyre menyseksjon viser nåværende innstillinger for sanntidssøk, skanning og automatisk oppdatering av anti-virusdatabasen og applikasjonsmoduler. Den gir også detaljerte kommentarer og råd fra Kaspersky Lab om hvordan du tilpasser innstillingene. For eksempel, dersom du manuelt oppdaterer din anti-virusdatabase, vil du varsles om at vi anbefaler automatiske oppdateringer.

Ved å klikke på lenkene i venstre menyseksjon av **Innstillinger** arkfanene kan du redigere alternativer for sanntidssøk, skanning og oppdatering av anti-virusdatabasen.

Du kan i tillegg redigere alternativer for karantenen - hvor mistenkelige objekter passerer. Til slutt kan du stille inn andre programalternativer fra lenken Utvidede innstillinger.

### 5.3.3. Brukerstøtte arkfanen

Under **Brukerstøtte** arkfanen finner du informasjon om Kaspersky Labs teknisk brukerstøtte og hvordan du kan få assistanse dersom du har problemer med programmet. Høyre menyseksjon viser informasjon om applikasjonen, lisensnøkkel og din datamaskins operativsystem - slik at du kan videreformidle denne informasjonen til brukerstøtte, om dette er nødvendig.



Bilde 5. Brukerstøtte arkfanen

Ved å klikke på lenkene i venstre menyseksjon kan du:

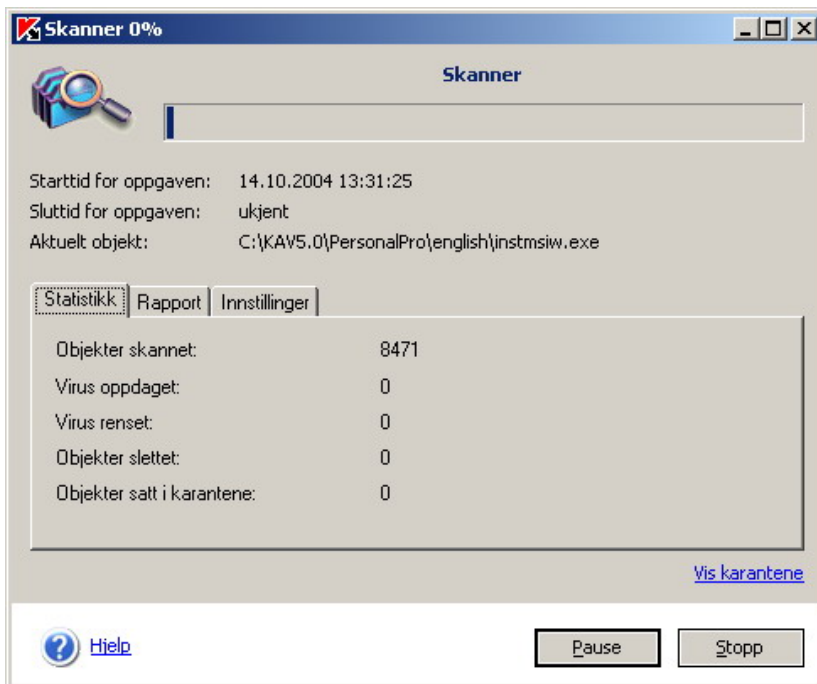
- sende spørsmål til Kaspersky Labs brukerstøtte
- send mistenkelige objekter til Kaspersky Lab for analyse
- fornye din lisens for Kaspersky Anti-Virus ved å installere ny lisensnøkkel

Seksjonen inneholder også følgende referanser:

- Hvordan... - generell referanse for programmet
- Hjelp - referanse om utførelse av oppgaver, og avansert hjelp
- Virusleksikon - lenke til [www.viruslist.com](http://www.viruslist.com), nettsted som inneholder detaljert informasjon om alle kjente skadelige programmer
- Kaspersky Labs hjemmeside - lenke til Kaspersky Labs hjemmeside

## 5.4. Skannevinduet

Når du starter en skanning for hele eller deler av din datamaskin, vil skannevinduet vises.



Bilde 6. Skannevinduet

Skannevinduet består av to deler:

- øverste del av vinduet inneholder informasjon om fremdrift for skanningen (i prosent), når skanningen startet, estimert sluttid og navn på objektet som skannes nå.
- nederste del av vinduet inneholder tre arkfaner: **Statistikk** (som viser resultatet av skanningen), **Rapport** (som inneholder detaljert informasjon om hendelser som oppstår under skanning) og **Innstillinger** (som inneholder en liste med innstillinger som er i bruk for skanningen).



Se også avsnittet [Behandle rapporter](#).

## 5.5. Applikasjonens referansesystem

Omfattende referanseinformasjon er tilgjengelig fra **Brukerstøtte** arkfanen i hovedvinduet ved å klikke på lenken [Hvordan...](#) fra venstre menyseksjon.

Når du trenger informasjon om hvordan du utfører oppgaver, kan du klikke på lenken [Hjelp](#) fra arkfanen **Brukerstøtte** i hovedvinduet. [Hjelp](#) inneholder detaljerte beskrivelser av nøkkelfunksjoner for anti-virusbeskyttelsesoppgaver som utføres av Kaspersky Anti-Virus og svar på OSS (ofte stilte spørsmål).

Dersom du har spørsmål om en bestemt dialogboks, kan du klikke på **<F1>** eller klikke [Hjelp](#) nederst i venstre hjørne av dialogboksen

---

# KAPITTEL 6. FOREBYGGING AV VIRUSINFEKSJON

Selv utprøvde og pålitelige beskyttelsestiltak kan ikke garantere en 100% beskyttelse mot datavirus og trojaner, men du kan selv redusere risikoen for virusangrep dramatisk ved å følge et par regler:

Tilsvarende helseproblemer, er en av hovedmetodene for å bekjempe virusinfeksjoner forebygging. For datamaskiner betyr dette at man må følge et par regler som reduserer risikoen for infeksjoner og ødeleggelse av data.

Her er hovedreglene for datasikkerhet, som hjelper å forebygge virusangrep:

**Regel 1:** hold din datamaskin beskyttet med anti-virusprograms og personlig brannmur. For å gjøre dette:

- Installer Kaspersky Anti-Virus Personal.
- Oppdater anti-virusdatabase daglig. I perioder med virusutbrudd bør du oppdatere flere ganger daglig - siden vi i slike perioder konstant oppdaterer databasene på oppdateringsserveren.
- Bruk anbefalte innstillinger for sanntidssøk. Sanntidsbeskyttelsen er aktivert umiddelbart etter at systemet starter opp, og forebygger viruspenetrasjon på din datamaskin.
- Bruk anbefalte innstillinger for skanning, og kjør regelmessig skanning minst en gang hver uke.
- Vi anbefaler at du også installerer Kaspersky Anti-Hacker for omfattende beskyttelse mens du surfer på Internett.

**Regel 2:** utøv forsiktighet når du kopierer nye data til din datamaskin:

- Skann alltid flyttbare medier (disketter, CD-ROM, minnekort etc.) etter virus før du bruker de.
- Vær forsiktig med e-postmeldinger. Åpne aldri vedlegg, selv fra kjente adresser, dersom du ikke venter vedlegget. Stol aldri på e-post som identifiserer seg selv som sendt av et anti-virusselskap.
- Vær forsiktig med data som lastes ned fra Internett. Når du får spørsmål om å laste ned programmer, sjekk sertifikatet som følger med nettstedet eller programmet.
- Dersom du laster ned en kjørbare fil fra Internett eller lokalnettverket, skann det med Kaspersky Anti-Virus før du kjører det.

- Velg nettsteder du besøker med sunn fornuft. Noen nettsteder inneholder skadelige skript eller Internett ormer.

**Regel 3:** Les alltid all informasjon som kommer fra Kaspersky Lab.

I de fleste tilfeller vil Kaspersky Lab advare brukere om nye virus lenge før de er på spredningstopp. Risikoen for infeksjoner er da stadig liten, og dersom du laster ned oppdateringer til anti-virusdatabasen, er du beskyttet mot angrepet.

**Regel 4:** Vær mistenksom når du mottar falske virusmeldinger - e-postmeldinger som påstår de er advarsler om virustrusler.

**Regel 5:** Regelmessig oppdater ditt operativsystem ved hjelp av Windows Oppdatering.

**Regel 6:** Kjøp alltid lisensierte versjoner av programvare fra autoriserte forhandlere.

**Regel 7:** Begrens antallet brukere som har tilgang til din datamaskin.

**Regel 8:** Minimer muligheten for tap av data ved en mulig infeksjon:

- Ta regelmessig sikkerhetskopi av dine data, slik at dersom du mister data lettvis kan gjenopprette sikkerhetskopiene. Distribusjonsdisketter, cd'er og andre medier med programvareinstallasjon og andre data bør oppbevares på en trygg plass.
- Lag alltid diskettet for gjenoppretting av systemet, slik at du kan starte med et "rent" operativsystem

## 6.1. Når trenger jeg å kjøre en virusskann?


Kaspersky Anti-Virus kan skanne hele datamaskinen eller en bestemt stasjon, mappe, fil eller ett e-postobjekt.



Under en full skanning, skannes ikke flyttbare medier eller nettverkstasjoner.

Selv om du, under en skanning, ikke oppdager virus, betyr ikke dette nødvendigvis at din datamaskin ikke har virus. Derfor vil Kaspersky Anti-Virus alltid sjekke om hele datamaskinen er skannet.

Under en full skanning skanner applikasjonen flere objekter lagret på din datamaskin enn under sanntidssøk. Dersom anbefaler vi at du skanner din datamaskin minst en gang hver uke - som forebyggende tiltak. Programmet vil varsle deg når det er på tide å starte en ny skann, og dersom hovedvinduet er

lukker, vil en varslingsmelding dukke opp med anbefalinger om tiltakt, ved ikonet  på oppgavelinjen. (Dersom du ikke har skrudd av varslingsmeldinger, se avsnittet [Utvidede innstillinger for Kaspersky Anti-Virus Personal](#))

For ytterligere informasjon kan du åpne hovedvinduet og se på skannestatus i høyre menyseksjon av **Beskyttelse** arkanen. Skannestatusen indikeres med følgende ikoner:



– Det er veldig viktig at du kjører en full skann av din datamaskin med en gang.



– Du burde kjøre en full skann av din datamaskin nå. Det er anbefalt at du gjenoppretter anbefalte innstillinger før du startet skanningen.



– Full skann gjennomføres regelmessig eller utføres nå.

Dersom det er påkrev, kan du også starte en full skann fra denne menyseksjonen ved å klikke på lenken [Skann nå](#).

Kaspersky Lab anbefaler at du starter regelmessig skanning automatisk (se avsnittet [Regelmessig skanning](#)). Status for full skanning vises uavhengig av om regelmessig skanning er aktivert eller ikke



#### **En komplett skanning etter virus er ikke utført.**

Det er ekstremt viktig at du [utfører en komplett skann](#) med en gang. Regelmessig skanning etter virus er aktivert. Du kan [endre intervall](#) for skanningen.

Bilde 7. Informasjon om behov for full skann.

## 6.2. Søkeinnstillinger i bruk

Etter installasjon av Kaspersky Anti-Virus, vil alle beskyttelsesoppgaver utføres med anbefalte innstillinger. Status for nåværende skanneinnstillinger vises i høyre menyseksjon av **Innstillinger** arkanen i hovedvinduet ved hjelp av følgende ikoner:



– Anbefalt beskyttelse for skanning er ikke i bruk.



– Anbefalte beskyttelse for skanning er i bruk.

Ved behov, kan du endre innstillingene. Du kan endre beskyttelsesnivået og spesifisere hvilke handlingsalternativer du ønsker utført dersom det oppdages misstenkelige eller infiserte objekter.



**Beskyttelsesnivået du aktiverer vil gjelde for ALLE TYPER av skanning, inkludert full skann av din datamaskin, valgte stasjoner, mapper, filer etc.**

Dersom du unnlater en bestemt stasjon fra skanningen (se avsnittet [Avanserte innstillinger for skanning](#)) vil denne stasjonen ikke skannes selv om du velger at den skal skannes (se avsnittet [Velg objekter som skal skannes](#)). Eneste unntak fra denne regelen er e-postkontoer for Microsoft Outlook og Microsoft Outlook Express. Dersom disse velges, vil de skannes uavhengig av om du har unntatt de fra skanning.



*For å endre beskyttelsesnivået og/eller handlingsalternativer ved oppdagelse av misstenkelige eller infiserte objekter:*

1. Klikk [endre innstillinger](#) i høyre menyseksjon av **Innstillinger** arkfanen eller [Innstillinger for skanning](#) i venstre menyseksjon.
2. I vinduet **Innstillinger for skanning**, velg hvilket beskyttelsesnivå du ønsker - som vil definere grundigheten av anti-virusbeskyttelsen på din datamaskin. Anbefalt nivå er standard. Du kan endre ved å bevege rullemenyen opp eller ned. Under følger en beskrivelse av hvert nivå - sammen med hvilke situasjoner som kan oppstå:

- **Maksimal beskyttelse** - grundig skanning av din datamaskin eller bestemte mapper, stasjoner eller filer.

Vi anbefaler at du bruker dette nivået dersom du misstenker at din datamaskin er infisert av virus. En detaljert beskrivelse av infeksjonssymptomer er tilgjengelig i avsnittet [Infeksjonssymptomer](#)

- **Anbefalt nivå** - skanner din datamaskin eller valgte objekt med innstillinger anbefalt av Kaspersky Labs eksperter.

Vi anbefaler å bruke dette nivået i en normal situasjon - siden det sikrer en optimal kombinasjon mellom skannehastighet og antall objekter som skannes.

- **Høy hastighet** - høy-hastighet anti-viruskanning av din datamaskin (inkludert minne og oppstartssektorer) eller av valgte objekter.

Dette beskyttelsesnivået sikrer maksimal skannehastighet grunnet reduksjonen i antall objekter som skannes.

Denne tabellen inneholder en oversikt over hvilke objekter som skannes i de forskjellige beskyttelsesnivåene. "+"-symbolet betyr at objektet skannes på dette nivået, mens "-"-symbolet betyr at objektet ikke skannes.

	Maksimal beskyttelse	Anbefalt nivå	Høy hastighet
Område valgt av bruker	+	+	+ <sup>3</sup>
Oppstartssektor, minne	+	+	+
OLE-objekter	+	+	+
Pakkede filer	+	+	+
Selvutpakkende arkiver	+	+	+
Objekter som kjøres ved systemoppstart	+	+	-
Arkiver	+	+	-
MS Outlook og MS Outlook Express e-postkontoer	+	+	-
E-postdatabaser og meldinger	+	-	-

For hvert av beskyttelsesnivåene kan du spesifisere unntak - en liste med objekter som ikke skal skannes. Uansett, vi anbefaler kun at du spesifiserer slike unntak dersom du har problemer med ytelsen av Kaspersky Anti-Virus, for eksempel dersom du opplever en dramatisk reduksjon i hastigheten av din datamaskin.

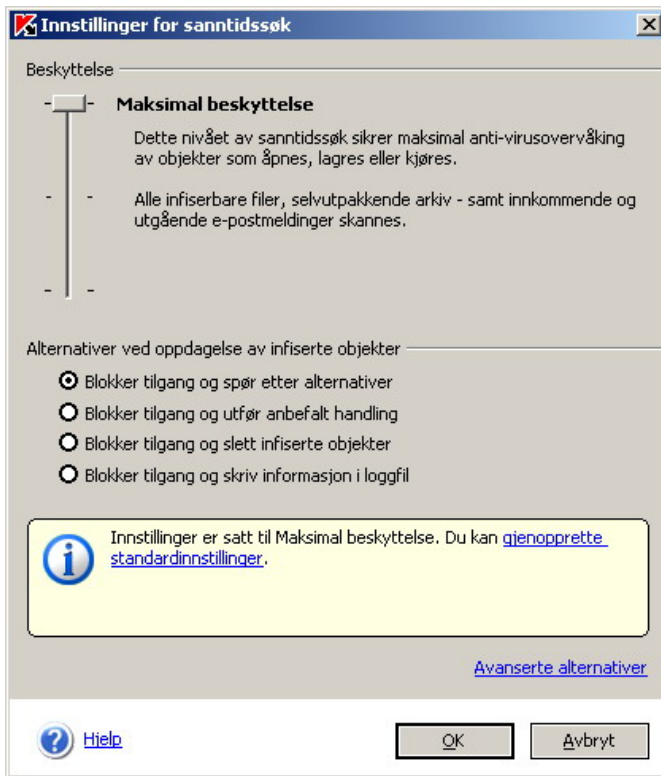
3. Spesifiser handlingsalternativer du ønsker utført dersom ett misstenkelig eller infisert objekt oppdages under skanning.



**Blokker tilgang og spør etter alternativer** - vil spørre om hvilke handlinger du ønsker utført. En liste med mulige alternativer vil

<sup>3</sup> Applikasjonen vil bare skanne mulig infiserbare filer.

vises, og ett av alternativene vil anbefales av Kaspersky Lab. Velg denne innstillingen dersom du er ved din datamaskin under skanning.



Bilde 8. Innstillinger for sanntidssøk

**Blokker tilgang og utfør anbefalt handling** - utfører handlingsalternativ anbefalt av Kaspersky Lab. Siden anbefalte alternativer alltid er velbalanserte, kan du velge dette alternativet i de fleste tilfeller. Anbefalte handlinger er som regel:

- rens *infiserte objekter*
- sette *misstenkelige eller infiserte objekter* i karantene

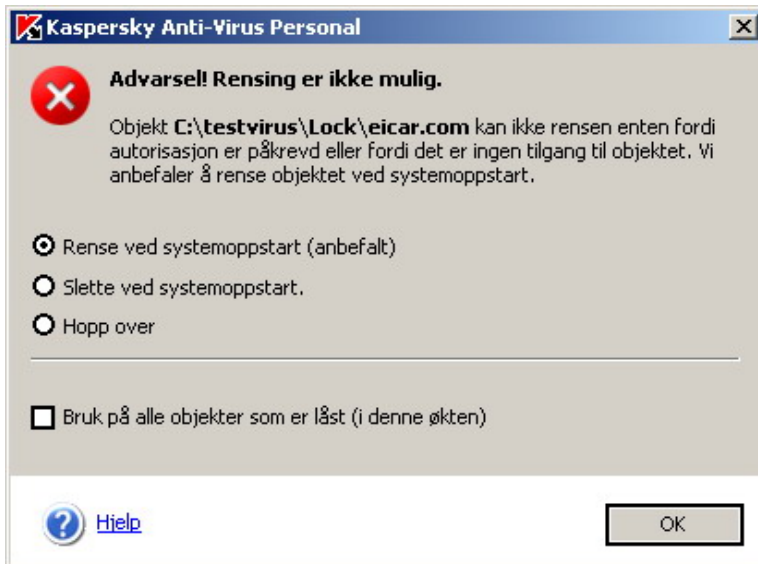


Etter en fil er plassert i karantene, kan det hende at en melding vises som varslar at objektet ikke kan slettes. Dette har sammenheng med at karanteneprosessen innebærer en fysisk flytting av objektet og deretter sletting av objektet fra sin opprinnelige plassering. I tillegg er det noen objekter (som f. eks. objekter i selvutpakkende arkiver) som ikke kan slettes under en slik prosess.

- slett skadelige programmer (*trojaner og ormer*) eller infiserte objekter som ikke kunne renses.
- **Blokker tilgang og slett infiserte objekter** - sletter infiserte objekter som oppdages under skanning uten å forsøke å rense de eller varsle brukeren. Dette alternativet er anbefalt hvis du er veldig sikker på at du ikke kan miste verdifull informasjon.
- **Blokker tilgang og skriv informasjon i loggfil** - vil kun rapportere om infiserte eller mistenkelige objekter som oppdages under skanning - uten å utføre noen handling på objektet. Dette alternativet er ikke anbefalt i de fleste tilfeller - siden alle infiserte eller andre skadelige objekter fortsatt vil være lagret på din datamaskin, og dermed nesten uten unntak bli utsatt for infeksjon.

I noen situasjoner kan ikke noen handlinger utføres på et objekt, for eksempel dersom et infisert objekt er i bruk av et annet program når det oppdages, og kan derfor ikke renses. I slike tilfeller vil en varslingsmelding vises med følgende forslag til handling:

- *rense ved systemoppstart*. Viser kun dersom objektet kan renses
- *slette ved systemoppstart*
- *hopp over* - utfører ingen handling på objektet, rapporterer om oppdagelse i loggfilen



Bilde 9 Rensing er ikke mulig.



For en vellykket behandling (rensing eller sletting) av objekter ved systemoppstart, må skanneprosessen fullføres før du starter om systemet. Dersom du avbryter skanningen, vil ikke objektene renses eller slettes.

## 6.3. Starte en full skann



For å starte en full skanning av din datamaskin:

klikk [Skann min datamaskin](#) i venstre menyseksjon av **Innstillinger** arkfanen

Når du har klikket på lenken, vil [Skannevinduet](#) vises. Dette vinduet viser fremdrift, starttid for skanningen, estimert sluttid og navnet på objektet som skannes nå

Du kan se detaljer om skannerresultater i rapporten

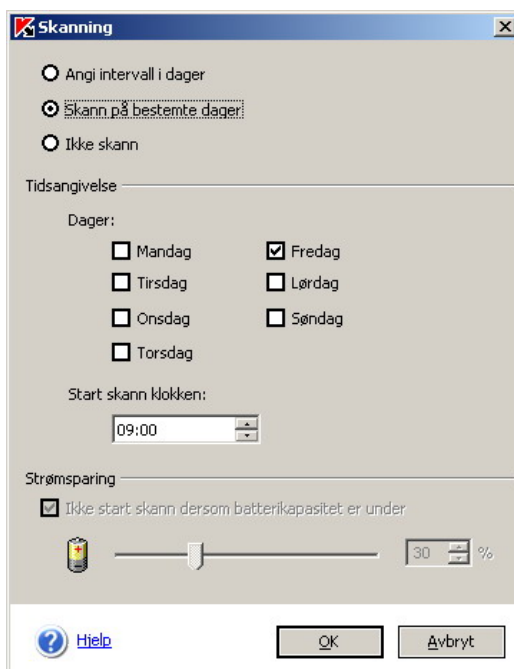
## 6.4. Regelmessig skanning

Du kan angi regelmessige intervaller for skanning - som også kan utføres på bestemte ukedager. For eksempel kan du velge å starte en full skanning ved lunsjtid.



*For å planlegge en regelmessig automatisk full skanning:*

1. Klikk Innstillinger for skanning i venstre menyseksjon av **Innstillinger** arkfanen.
2. Når vinduet **Innstillinger for skanning** vises, klikk Tidsplanlegging for skanning.
3. Da vises vinduet **Tidsplanlegging for skanning**, og du kan angi hvilke alternativer du ønsker:



Bilde 10. Tidsplanlegging for skanning

- Angi intervall i dager** - utfører anti-viruskanning med et bestemt antall dagers mellomrom. Standardinnstillinger er daglig skanning klokken 18:00. Dersom du ønsker å endre innstillingene, velg Hver alternativet, og intervallet i dager i feltet som står til høyre. Angi starttid for skanningen i Start skann klokken feltet.
- Skann på bestemte dager** - angi ukedager du ønsker skanningen på. Standardinnstillinger er ukentlig, hver fredag klokken 18:00. Dersom du ønsker å endre innstillingene, velg Dager i Tidsangivelse seksjonen, og angi starttid for skanningen i Start skann klokken feltet.
- Ikke start skann dersom batterikapasitet er under** - for bærbare datamaskiner: avbryter skanningen dersom batterikapasiteten er mindre en angitte minstekrav. Du kan endre verdien ved å dra bryteren (angis i prosent).

4. Klikk **OK**.

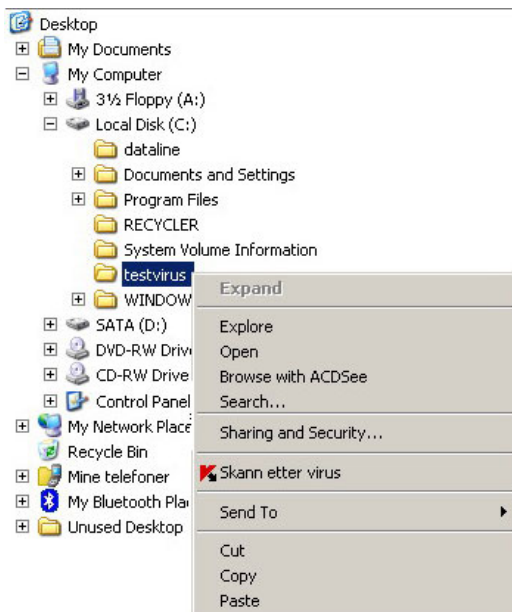
## 6.5. Velg objekter som skal skannes

Noen ganger kan du ha behov for å skanne enkelte objekter, i stedet for å skanne hele datamaskinen. Slike objekter kan for eksempel være: en lokal stasjon med programfiler og spill, e-postdatabaser du har tatt med fra kontoret eller ett arkiv som kom vedlagt en e-postmelding. Du kan velge enkeltobjekter som skal skannes enten fra Kaspersky Anti-Virus eller fra vanlige Windows-verktøy (for eksempel, **Windows Utforsker**, **Min Datamaskin**, etc.).



*Hvordan skanne et objekt ved bruk av standard Windows-verktøy*

Velg og høyreklikk objektet du ønsker å skanne. Når hurtigmenyen vises, velg **Skann etter virus**



Bilde 11. Skanne et objekt ved hjelp av Windows Utforsker

For å velge og skanne objekter ved hjelp av Kaspersky Anti-Virus, vennligst følg instruksjonen under:



*Hvordan skanne et objekt ved bruk av Kaspersky Anti-Virus Personal :*

Klikk Skann objekter i venstre menyseksjon av **Beskyttelse** arkfanen.

Da vil **Velg objekter som skal skannes** vinduet vises, med en liste over objekter som kan skannes.



Bilde 12. Valg av objekter som skal skannes

Standardlisten som vises inneholder følgende objekter:

- flyttbare medier, inkludert disketter er CD-ROM
- lokale stasjoner
- Microsoft Outlook og Microsoft Outlook Express e-postkontoer
- Mappen: **Mine dokumenter**

For å legge til nye objekter, klikk **Legg til**. I ett nytt vindu kan du bla gjennom etter filer eller mapper du ønsker å legge til. Alle objekter som legges til vil lagres i listen for fremtidig bruk.

For å slette et objekt fra listen, velg objektet ved å markere  og klikk **Slett**. Du kan kun slette objekter fra listen som du selv har lagt til. Alle objekter som er i startlisten kan ikke fjernes



Velge og skanne objekter fra listen:

1. Velg (marker) objekter du ønsker å skanne fra listen
2. Klikk **Skann** for å starte skanning

Uavhengig av hvordan programmet ble startet (fra Kaspersky Anti-Virus eller fra Windows hurtigmeny), vil **Skannevinduet** (se bilde 6) vises..

Alle resultater lagres, og kan behandles i rapportene.

## 6.6. Skanning i arkiver

Kaspersky Anti-Virus skanner arkiver dersom beskyttelsesnivåene **Maksimal beskyttelse** eller **Anbefalt nivå** er valgt, og dersom disse arkivene ikke er unntatt fra skanning (se avsnittet Avanserte innstillinger for skanning).



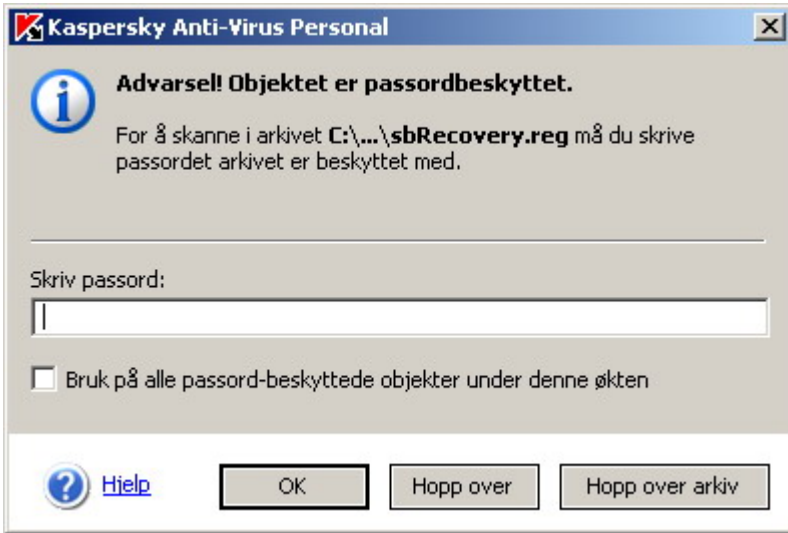
Kaspersky Anti-Virus skanner alle objekter i arkiver, men kan kun renses i zip, arj, cab og rar formater.

Selvutpakkende arkiver kan ikke renses. Dersom et virus oppdages i et slikt arkiv, vil arkivet slettes.

Dersom et arkiv eller objekt i arkivet er passordbeskyttet, vil en varslingsmelding som spør etter passordet vises før skanningen fortsetter.



You Du kan aktivere eller deaktivere spørsmål om passord ved å markere  **Ikke spør etter passord under skanning i objekter** fra Avanserte alternativer i Innstillinger for skanning.



Bilde 13. Spørsmål om passord under skanning

I feltet **Skriv passord** kan du skrive passordet arkivet eller objektet er beskyttet med, og deretter klikke **OK**. Arkivet, og alle objekter i arkivet, vil skannes med dette passordet.



Når objekter i arkiver behandles, pakker Kaspersky Anti-Virus Personal ut arkivet til en midlertidig mappe, skanner objektene, behandler dem, pakker de tilbake i et nytt arkiv med samme navn og plasserer dette arkivet tilbake til plasseringen for det originale arkivet. Tilsvarende prosedyre brukes for behandling av passordbeskyttede objekter i arkivet. Husk at objekter som er behandlet da pakkes i ett nytt arkiv uten å bruke passord.

Dersom et nytt passordbeskyttet arkiv blir oppdaget i arkivet som behandler, vil Kaspersky Anti-Virus Personal automatisk benytte angitte passord for det første arkivet for å behandle det andre arkivet. Du får kun spørsmål om passord dersom passordet ikke er gyldig for dette arkivet.

Dersom du ikke ønsker å skanne et bestemt passordbeskyttet objekt i arkivet, kan du klikke **Hopp over**.

Dersom du ikke vet passordet, kan ikke programmet skanne dette passordbeskyttede arkivet eller objektene i arkivet. Vi anbefaler at du da klikker **Hopp over** arkiv.

Dersom du markerer  **Bruk på alle passordbeskyttede objekter under denne økten**, vil passordet benyttes på alle passordbeskyttede objekter:

For eksempel: Dersom du markerer denne boksen, og klikker **Hopp over** arkiv knappen, vil programmet ikke skanne passordbeskyttede arkiv under denne skanningen.

Dersom du skriver et passord, markerer boksen og så klikker **OK** vil dette passordet benyttes på alle passordbeskyttede objekter under denne skanningen. Dersom passordet ikke er gyldig for et bestemt objekt, vil dette objektet ikke skannes.

---

# KAPITTEL 7. SKANNE EN CD ELLER EN DISKETT

Din datamaskin kan enkelt infiseres av virus på en diskett, CD eller ett annet flyttbart medie. Dersom en diskett (eller en oppstarts-CD) du har brukt er infisert av et oppstartsvirus, og du har startet systemet fra dette mediet - kan det medføre de alvorligste følger for ditt system.

Vi anbefaler at du skanner alle flyttbare medier før du bruker de.

Du kan skanne flyttbare medier enten fra hovedvinduet i Kaspersky Anti-Virus, eller fra hurtigmenyen i Windows som du har tilgang til fra **Windows utforsker**, **Min datamaskin** etc.



*Å skanne flyttbare medier for virus fra Windows hurtigmeny:*

Velg og høyreklikk stasjonen (du kan velge på CD-ROM og disketter samtidig). Når hurtigmenyen vises, velg **Skann etter virus**.(se Bilde 11)



*Å skanne en CD-ROM eller diskett for virus fra hovedvinduet i Kaspersky Anti-Virus::*

1. Sett inn diskett eller CD-ROM (programmet kan skanne begge stasjonene samtidig).
2. Klikk Skann flyttbare medier i venstre menyseksjon av **Beskyttelse** arkfanen.

*eller*

Ved å bruke Skann objekter, gå til Velg objekter som skal skannes, marker CD-ROM og diskett, og klikk Skann.

Du kan overvåke skanneprosessen i **Skannevinduet** (se bilde 6) som vises umiddelbart etter du starter skanningen.

Dersom du velger kun ett flyttbart medie du vil skanne vil du etter skannet er fullført bli varslet om du ønsker å sette inn neste medie for skanning.



#### Viktig informasjon om programmets funksjoner:

- dersom CD-en eller disketten er tom, vil ikke mediet skannes. Ingen melding vil vises.
- en CD, diskett eller ett annet flyttbart medie som settes inn i stasjonen etter skanning er startet vil ikke skannes.
- Dersom du løser ut CD eller diskett, eller kobler fra stasjonen, når skanning pågår - vil applikasjonen skrive feilmeldingen i rapporten, men ingen melding vil vises. Etter dette vil det neste flyttbare mediet skannes, dersom det finnes på din datamaskin.

Hver gang ett flyttbart medie kobler til systemet (dvs. når er stasjon oppdages av systemet som ny maskinvare) vil det bli skannet for oppstartsvirus.

---

# KAPITTEL 8. INNSTILLING AV SANNTIDSSØK

Sanntidsbeskyttelse av din datamaskin betyr at Kaspersky Anti-Virus konstant overvåker potensielt usikre handlinger som utføres på din datamaskin. Applikasjonen skanner etter virus i følgende objekter: i filer som åpnes eller lagres (etter du har endret de), i meldinger du sender eller mottar, i filer som skal kjøres, i skript som skal kjøres i Microsoft Internet Explorer. Når en hvilken som helst av disse handlingene blir forsøkt utført, vil Kaspersky Anti-Virus først blokkere tilgangen (stoppe kjøringen), deretter skanne objektet - og så, avhengig av skanneresultat, enten tillate eller nekte handlingen, eller vise en varslingsmelding.

## 8.1. Sjekke beskyttelsesstatusen

Nåværende sanntidsbeskyttelse vises i høyre menyseksjon av Beskyttelse (se bilde 3) arkfanen i hovedvinduet.

Status for sanntidsbeskyttelsen vises med følgende ikoner:



– Sanntidssøk er aktivert. Beskyttelse er satt til Anbefalt nivå.



– Sanntidssøk er aktivert. Beskyttelse tilsvarer ikke Anbefalt nivå.



– Sanntidssøk er ikke aktivert eller virker ikke. Dersom beskyttelsen er deaktivert, anbefaler vi at du aktivere den på nytt. Dersom beskyttelsen ikke virker, anbefaler vi at du sjekker alle innstillinger for sanntidssøk (se avsnittet Avanserte alternativer for sanntidssøk) og deretter aktiverer den.

## 8.2. Spesifisering av handlinger og innstilling av beskyttelsesnivå

Standard beskyttelsesnivå for Kaspersky Anti-Virus er **Anbefalt nivå**. Dette nivået blokkerer tilgang for alle infiserte objekter, skadelige programmer "malware" (ormer, trojanske programmer) og misstenkelige objekter som åpnes for lesing, skriving eller kjøring, og viser en varslingsmelding som spør etter handlingsalternativer.



Vær oppmerksom på at arkiver, e-postdatabase og e-post i ren tekst **IKKE SKANNES** i sanntidssøk! Ett unntak er selvutpakkende arkiver, som skannes dersom **Maksimal beskyttelse** er aktivert.

Når sanntidssøk er aktivert, kan du velge både beskyttelsesnivået du ønsker, og hvilke handlingsalternativer du ønsker skal utføres når ett misstenkelig eller infisert objekt oppdages.



*Å konfigurere applikasjonen når skadelig objekt oppdages:*

1. klikk Innstillinger for sanntidssøk i venstre menyseksjon av **Innstillinger** arkfanen eller endre innstillinger i statusområdet av **Beskyttelse** arkfanen.
2. Når dialogboksen Innstillinger for sanntidssøk vises, kan du velge nivået du ønsker. Ved å endre beskyttelsesnivået kan du selv velge hastigheten på skanning, og antallet objekter som skal skannes. Desto færre objekter som skannes, jo raskere vil skanningen utføres.



Vær oppmerksom på at arkiver ikke skannes eller renses i sanntidssøk. For å skanne og rense arkiver må du benytte skanning.



Bilde 14. Innstillinger for Sanntidssøk

### Kaspersky Anti-Virus ber deg velge ett av tre beskyttelsesnivå:

- **Maksimal beskyttelse** - dette nivået sikrer maksimal overvåking av objekter som åpnes, lagres eller kjøres.
- **Anbefalt nivå** - dette nivået er anbefalt av Kaspersky Lab. På dette nivået skannes samme type objekter som på nivået Maksimal beskyttelse, med unntak av selvutpakkende arkiver og utgående e-postmeldinger.
- **Høy hastighet** - dette nivået sikrer god ytelse på din datamaskin mens du jobber med programmer som krever mye minnebruk, fordi antallet objekter som skannes er mindre.

Denne tabellen inneholder en oversikt over hvilke objekter som skannes i de forskjellige beskyttelsesnivåene. "+"-symbolet betyr at objektet skannes på dette nivået, mens "-"-symbolet betyr at objektet ikke skannes

	Maksimal beskyttelse	Anbefalt nivå	Høy Hastighet
<b>Filer som akn infiseres</b>	+	+	+
<b>Oppstartssektorer</b>	+	+	+
<b>Pakkede filer</b>	+	+	+
<b>OLE objekter</b>	+	+	+
<b>Innkommende e-postmeldinger<sup>4</sup></b>	+	+	+
<b>Utgående e-postmeldinger<sup>5</sup></b>	+	-	-
<b>Selvutpakkende arkiver<sup>6</sup></b>	+	-	-
<b>E-postdatabaser og meldinger</b>	-	-	-

For hvert av beskyttelsesnivåene kan du spesifisere *unntak* - en liste med objekter som ikke skal skannes. Uansett, vi anbefaler kun at du spesifiserer slike unntak dersom du har problemer med ytelsen av Kaspersky Anti-Virus, for eksempel dersom du opplever en dramatisk reduksjon i hastigheten av din datamaskin.

3. Spesifiser handlingsalternativer som skal utføres ved oppdagelse av infiserte eller misstenkelige objekter:

---

<sup>4</sup> Innkommende POP3 e-post

<sup>5</sup> Utgående SMTP e-post

<sup>6</sup> Bare den kjørbare delen av det selvutpakkende arkivet skannes.

- **Blokker tilgang og spør etter alternativer** - vil spørre om hvilke handlinger du ønsker utført. En liste med mulige alternativer vil vises, og ett av alternativene vil anbefales av Kaspersky Lab.

Dersom du ikke har spesifisert et alternativ innen 30 sekunder, vil anbefalt handling bli utført på dette objektet. Hver type av oppdagede objekter har sin egen anbefalte handling. For eksempel, for infiserte objekter er anbefalt handling **Rense**. Ved siden av alternativene vil du på ett alternativ se teksten **Anbefalt**.

En liste med mulige anbefalte handlinger er:

- *rens* infiserte objekter
- sette misstenedelige eller objekter infiserte med virus eller virusmodifikasjon i *karantene*



Etter en fil er plassert i karantene, kan det hende at en melding vises som varslers at objektet ikke kan slettes. Dette har sammenheng med at karanteprosessen innebærer en fysisk flytting av objektet og deretter sletting av objektet fra sin opprinnelige plassering. I tillegg er det noen objekter (som f. eks. objekter i selvutpakkende arkiver) som ikke kan slettes under en slik prosess.

- *slett* skadelige programmer (trojaner eller ormer) eller infiserte objekter som ikke kan renses
- *hopp over* - utfører ingen handling på objektet, rapporterer om oppdagelse i loggfilen.



Dersom du ønsker å sette et infisert objekt i karantene, velg Hopp over og plasser objektet i karantenen manuelt (se avsnittet *Objekter i karantene*).

- **Blokker tilgang og utfør anbefalt handling** - blokkerer tilgang til objektet og utfører anbefalt handling. Anbefalt handling for infiserte objekter er *Rense*, for mulig infiserte objekter er det *Plasser i karantene* og for trojanske hester og ormer er det *Slett*.
- **Blokker tilgang og slett infiserte objekter** - sletter infiserte objekter som oppdages under skanning uten å forsøke å renses de eller varslinger.

- **Blokker tilgang og skriv informasjon i loggfil** - vil kun rapportere om infiserte eller mistenkelige objekter som oppdages under skanning - uten å utføre noen handling på objektet

I noen situasjoner kan ikke noen handlinger utføres på et objekt, for eksempel dersom et infisert objekt er i bruk av et annet program når det oppdages, og kan derfor ikke renses. I slike tilfeller vil en varslingsmelding vises med følgende forslag til handling:

- *rens* ved systemoppstart. Viser kun dersom objektet kan renses
- *slette* ved systemoppstart
- *hopp over* - utfører ingen handling på objektet, rapporterer om oppdagelse i loggfilen



Vær oppmerksom på at handlingsalternativene ikke gjelder for e-postmeldinger eller skadelige skript:

- Ved oppdagelse av infiserte eller mulig infiserte e-postmeldinger, blir anbefalt handling utført uten ytterligere bekreftelse fra brukeren.
- Ved oppdagelse av skadelige skript, blir du alltid varslet og må selv velge hvilken handling du ønsker å utføre.

---

# KAPITTEL 9. BESKYTTE E-POST MOT VIRUS

Kaspersky Anti-Virus gir deg sanntidsbeskyttelse av innkommende og utgående e-postmeldinger.



*Å beskytte din e-post mot virus:*

Aktiver sanntidssøk og sjekk at  **Deaktiver e-postsøk i Avanserte alternativer** ikke er markert..

Følgende regler gjelder for Kaspersky Anti-Virus' behandling av e-postmeldinger

- Din e-post er beskyttet mot virus uavhengig av hvilken e-postklient<sup>7</sup> du bruker<sup>1</sup>. Alle innkommende og utgående e-postmeldinger skannes så raskt de mottas eller sendes.
- Ved oppdagelse av infisert objekt i en e-postmelding, vil anbefalt handling bli utført for hvert objekt: Kaspersky Anti-Virus vil prøve å rense objektet. dersom ikke rensing er mulig vil objektet slettes fra meldingen.
- Dersom du bruker e-posttjenester på internettservere gjennom en nettleser, for eksempel gjennom Microsoft Internet Explorer, vil Kaspersky Anti-Virus skanne vedleggene når du åpner de eller lagrer de lokalt på din datamaskin.

E-postdatabaser importert fra andre datamaskiner - som ikke er oppkoblet, kan skannes ved å starte full skanning.

---

<sup>7</sup> Kaspersky Anti-Virus® Personal tilbyr sanntidssbeskyttelsen for all innkommende POP3 og utgående SMTP e-post meldinger.



Å skanne Microsoft Outlook eller Microsoft Outlook Express e-postkontoer:

1. sjekk at  **Deaktiver e-postsøk i Avanserte alternativer** ikke er markert.
2. klikk **Skann objekter** i venstre menyseksjon av **Beskyttelse** arkfanen.
3. I dialogboksen Velg objekter som skal skannes, marker boksen  **E-postkontoer**.
4. klikk **Skann**

Da vil alle Microsoft Outlook og Microsoft Outlook Express e-postdatabaser og e-postfiler skannes.



Som et resultat av behandling av Microsoft Outlook og Microsoft Outlook Express e-postdatabaser, vil alltid dato og klokkeslett for siste endring forandres, uavhengig av handlingsalternativ som utføres.



Å skanne e-postdatabaser for andre formater (for eksempel TheBat) eller databaser som du har på din harddisk (som du kan ha tatt med fra kontoret),


1. klikk **Skann objekter** i venstre menyseksjon av **Beskyttelse** arkfanen.
2. I dialogboksen **Velg objekter som skal skannes**, velg mappe eller stasjon hvor databasene er lagret
3. Klikk **Skann**.

---

# KAPITTEL 10. BEHANDLING AV INFISERTE OG MISSTENKELIGE OBJEKTER

Handlinger som utføres av Kaspersky Anti-Virus ved oppdagelse av infiserte eller misstenkelige objekter, avhenger av hvilke innstillinger du har valgt for sanntidssøk og skanning. Her vil vi beskrive situasjoner hvor Kaspersky Anti-Virus tilbyr flere mulige handlinger som kan utføres på objektene som oppdages.

Disse situasjonene oppstår når du har valgt følgende handlingsalternativer ved oppdagelse av infiserte eller misstenkelige objekter:

- Sanntidssøk:
  -  **Blokker tilgang og spør etter alternativer**
- Skanning:
  -  **Spør etter alternativer**

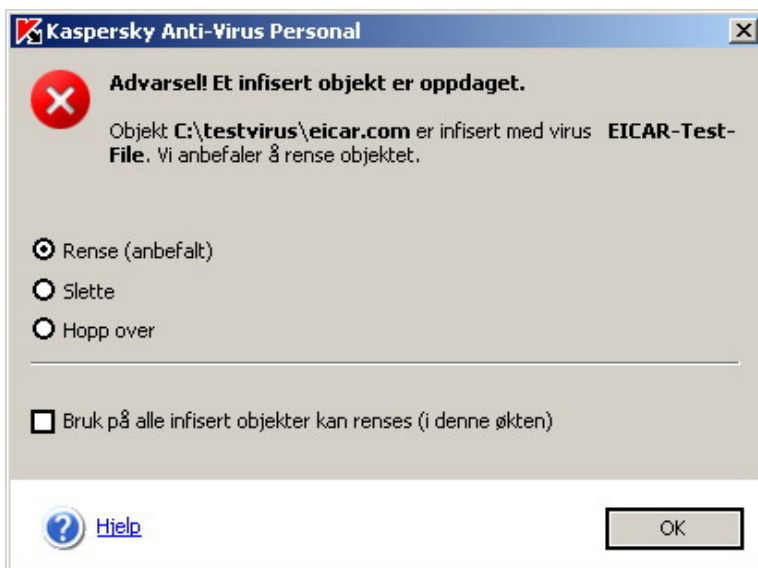
Ved oppdagelse av ett infisert eller misstenkelig objekt, vil en varslingsmelding (se Bilde 2) vises med følgende innhold:

- en detaljert beskrivelse av objektet, med en indikasjon på hvilket virus som kan ha infisert objektet - eller navnet på skadeprogrammet "malware", dersom det er et skadelig program;
- en liste med mulige handlinger som kan utføres på dette objektet. Listen har alltid ett alternativ anbefalt av Kaspersky Lab, som er merket med ordet "Anbefalt". Avhengig av hvilken type objekt som er oppdaget, kan du velge mellom følgende handlingsalternativer:
  - **Rense**- forsøker å rense det infiserte objektet dersom en behandling er mulig
  - **Slett** - sletter det infiserte eller mulig infiserte objektet
  - **Hopp over** - utfører ingen handling, skriver informasjon om objektet i rapporten
  - **Sette i karantene** - setter det misstenkelige objektet i karantene, slik at du siden kan sjekke, gjenopprette, slette eller sende det til

Kaspersky Lab for analyse (se avsnittet **Behandle objekter i karantene** ).

Du kan også velge handling som skal brukes på alle objekter med samme status, ved å markere boksen **Bruk på alle infiserte objekter....** Da vil for eksempel alle infiserte objekter som kan renses bli renses, dersom du markerer  **Bruk på alle infiserte objekter som kan renses (i denne økten)**.

Dersom du lukker dette vinduet ved å klikke  øverst i høyre hjørne, vil handlingen **Hopp over** bli brukt.



Bilde 15. Melding om oppdagelse av infisert objekt

---

# KAPITTEL 11. FORNYELSE AV LISENS

Du må ha en *lisensnøkkel* for å bruke Kaspersky Anti-Virus. Lisensnøkkelen gjør det mulig for deg å bruke programmet fra du har installert den i programmet.



**Kaspersky Anti-Virus VIRKER IKKE uten en lisensnøkkel!**

Når din lisens er utløpt, vil stadig Kaspersky Anti-Virus opprettholde sin funksjonalitet (altså fungere normalt) bortsett fra at du ikke kan oppdatere anti-virusdatabasen og applikasjonsmodulene. Du vil stadig kunne skanne din datamaskin og e-post for virus, og rense infiserte objekter. Du vil kun ha muligheten til å benytte en utdatert database som er fra den dato din lisens utløp. Derfor garanterer vi ikke 100% beskyttelse mot nye virus som oppdages etter din Kaspersky Anti-Viruslisens utløper.

For å unngå mulige infeksjoner av din datamaskin, anbefaler vi å fornye din Kaspersky Anti-Viruslisens.

Kaspersky Anti-Virus varsler den om lisensperiodens utløp to uker for utløpsdatoen. En varselsmelding vil vises hver gang du startet programmet i denne perioden



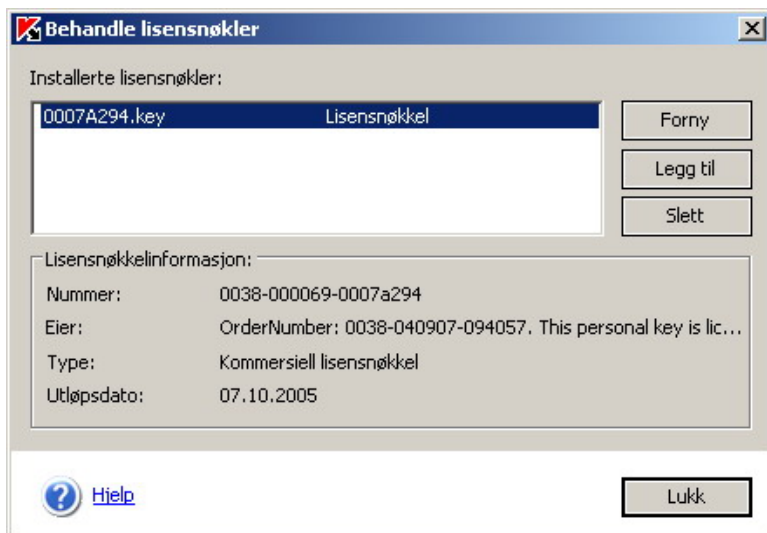
*For å fornye din lisens, må du kjøpe og installere en ny lisensnøkkel for Kaspersky Anti-Virus Personal:*

- Du kan skaffe deg en ny nøkkel ved å klikke på **Forny** i vinduet **Behandle lisensnøkler**, og følge instruksjonene på nettsiden
- Kontakte forhandleren du kjøpte den originale lisensnøkkelen fra.

Når du har kjøpt din nye lisensnøkkel, vil du motta denne på e-post eller motta en lenke til nedlastingssted. Last ned nøkkelen og lagre den på din datamaskin.

Installer den nye nøkkelen slik:

- klikk Lisensnøkler i venstre menyseksjon av **Brukerstøtte** arkfanen.
- Etter at vinduet **Behandle lisensnøkler** vises, klikk **Legg til** og velg den nye lisensnøkkelen ved hjelp av standard Windows **Velg** dialogboks



Bilde 16. Behandle lisensnøkler

---

# KAPITTEL 12. NEDLASTING AV OPPDATERINGER

For å holde Kaspersky Anti-Virus Personal oppdatert mot nye virus må programmet få oppdatere anti-virusdatabasen og applikasjonsmodulene på regelmessig basis.



**Regelmessig oppdatering av anti-virusdatabasen** sikrer den beste beskyttelse for din datamaskin. Nye virus oppdages daglig, og Kaspersky Lab overvåker og identifiserer disse truslene hele døgnet. Nye virusdefinisjoner blir hver time plassert på oppdateringsserverene til Kaspersky Lab og tilgjengelig for nedlasting. Vi anbefaler at du holder din anti-virusdatabase regelmessig oppdatert, minst en gang hver 12 time, og under virusutbrudd så ofte som mulig.

For å oppdatere din anti-virusdatabase, last ned oppdateringer via Internett fra Kaspersky Lab's oppdateringsservere, eller fra lokal mappe på din datamaskin (se seksjon under).

Oppdateringer kan enten lastes ned automatisk eller manuelt. Datamaskinen må være tilkoblet Internett for at oppdateringene skal kunne lastes ned. Oppdateringene blir automatisk installert når nedlastingen er ferdig

## 12.1. Når bør du laste ned oppdateringer

Programmet vil gi deg beskjed når du trenger å oppdatere din anti-virusdatabase. Du kan også lese anbefalinger og informasjon om databasen i høyremenyen på **Beskyttelse** arkfanen.

De følgende symbolene brukes for å informere om statusen på din anti-virusdatabase:



– din anti-virusdatabase har nylig blitt oppdatert.



– din anti-virusdatabase må oppdateres. Dersom oppdatering ikke er mulig fordi din lisens har utløpt, vil tilbys informasjon om fornyelse av lisensen.



– du må oppdatere din anti-virusdatabase med en gang! Den er enten veldig gammel eller mangler!

## 12.2. Laste ned oppdateringer via Internett

Kaspersky Lab oppdaterer anti-virusdatabasen på oppdateringsserveren hver time.

Kaspersky Lab's oppdateringsservere støtter både HTTP og FTP for nedlasting



*For å forsikre deg om at din anti-virusdatabase alltid er oppdatert, må du følge beskrivelsen under:*

1. Klikk Innstilling for oppdatering i venstremenyen på **Innstillinger** arkfanen.
2. Velg en av de følgende alternativene i **Oppdateringstype** menyen:  
*fra Internett, standard database* - anti-virusdatabasen kan gjenkjenne og rense alle kjente forekomster av ondsinnet kode.  
*fra Internett, utvidet database* - standard database pluss en ekstra database som lar Kaspersky Anti-Virus oppdage programmer som er definert som skadelige (fjernstyring, overvåking av din datamaskin m.v).



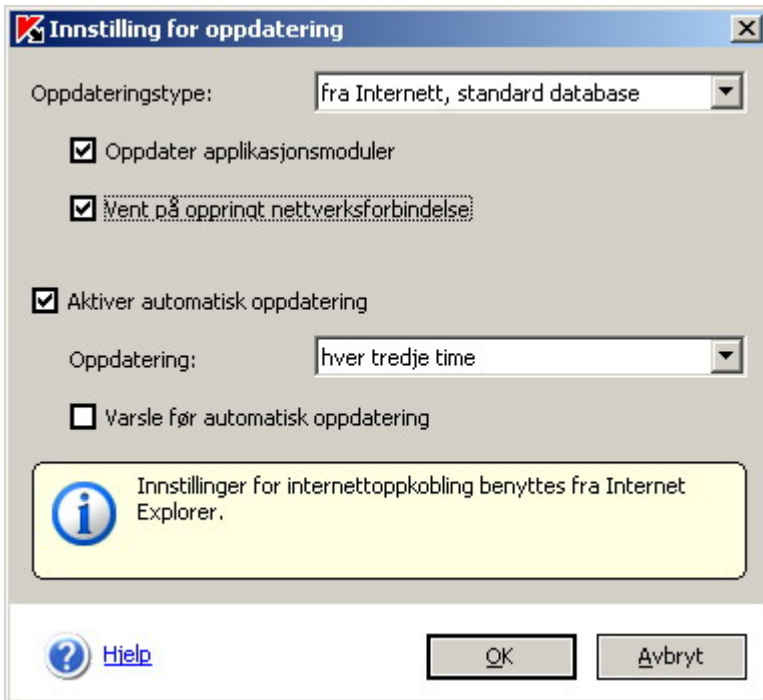
**Den standard anti-virusdatabasen gir beskyttelse mot virusangrep. Ved å bruke den utvidete databasen kan programmet bli noe tregere.**

3. Dersom du bruker en nettverksforbindelse hvor du må manuelt ringe opp koblingen, og du ikke vil programmet skal forsøke å koble seg til Internett automatisk, marker  **Vent på oppringt nettverksforbindelse.**



**Denne innstillingen er benyttet for at programmet skal kunne oppdatere anti-virusdatabasen automatisk:**

4. Klikk **OK**.



Bilde 17. Innstillinger for oppdatering



Nettverksforbindelsen vil benytte standard oppkoblingsregler (de samme som for Internet Explorer). For å forandre denne innstillingen, velg **Start** → **Kontrollpanel** → **Alternativer for Internett** → **Tilkoblinger**.

## 12.3. Laste oppdateringer fra en lokal mappe

Dersom du ikke har tilgang på oppdateringsserverene fra Kaspersky Lab (for eksempel hvis du ikke har tilgang på Internett), kan du ta kontakt med din lokale forhandler av Kaspersky Anti-Virus - eller ring +7 (095) 797-87-00 og spør om nærmeste forhandler. Forhandleren kan skaffe deg de siste anti-virusdatabasene på disketter eller CD-ROM.



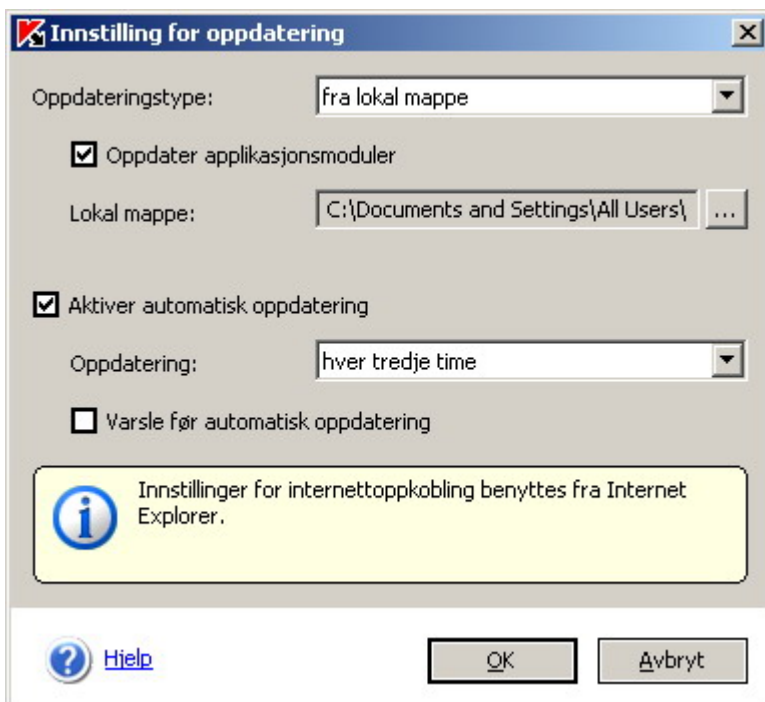
Når du bestiller oppdateringer til anti-virusdatabasen, husk å si ifra hvilken type virusdatabase (vanlig eller utvidet) du ønske.

Når du mottar oppdateringene på diskett eller CD-ROM, pakk ut filene til en lokal mappe.



For å laste oppdateringene til anti-virusdatabasen fra en lokal mappe:

1. Klikk Innstillinger for oppdatering i venstremenyen på **Innstillinger** arkfanen.
2. I **Oppdateringstypen**, velg fra **lokal mappe**.
3. Spesifiser plasseringen hvor oppdateringene er lagret.
4. Klikk **OK**.



Bilde 18. Innstillinger for oppdatering

## 12.4. Oppdatere Kaspersky Anti-Virus Personal applikasjonsmoduler

I tillegg til å oppdatere din anti-virusdatabase, kan du også oppdatere Kaspersky Anti-Virus applikasjonsmoduler. Applikasjonsmoduler oppdateres når det er behov for det (nye komprimeringsmetoder for filer som kan inneholde virus, m.v).

Du kan oppdatere applikasjonsmodulene fra en oppdateringsserver, eller fra en lokal mappe. For å tillate oppdateringer av applikasjonsmoduler marker  **Oppdater applikasjonsmoduler** i Innstillinger for oppdatering (se Bilde 18).



Dersom du ønsker å oppdatere applikasjonsmoduler fra en lokal mappe, må du motta disse fra din leverandør av Kaspersky Anti-Virus.

## 12.5. Automatiske oppdateringer

Kaspersky Lab anbefaler at du benytter deg av den automatisk oppdateringsfunksjonen i programmet. Videre anbefales det å oppdatere anti-virusdatabasen hver 12. time, og under virusutbrudd så ofte som mulig.



*For å automatisk laste ned oppdateringer til din anti-virusdatabase:*

1. Klikk **Innstillinger for oppdateringer** i venstremenyen på **Innstillinger** arkfanen.
2. Marker  **Aktiver automatiske oppdateringer**.
3. Velg oppdateringsfrekvensen fra listen.

## 12.6. Oppdateringer



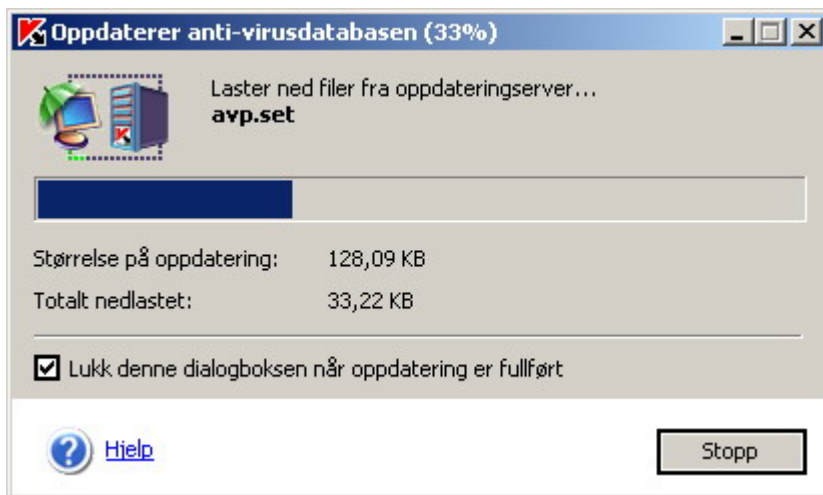
*For å laste ned oppdateringer til din anti-virusdatabase:*

klikk Oppdater nå i venstremenyen på **Beskyttelse** arkfanen.

Manuell eller automatisk oppdatering kan bare starte hvis datamaskinen din er tilknyttet Internett. Prosessen vil ikke starte dersom datamaskinen ikke er tilknyttet Internett.

Oppdateringsprosessen består av tre deler:

1. Programmet mottar en liste over oppdateringer og størrelsen på oppdateringene fra oppdateringsserveren.
2. Din anti-virusdatabase og applikasjonsmoduler blir sammenlignet mot informasjonen hentet fra oppdateringsserveren. Dersom du har den nyeste anti-virusdatabasen installert på din maskin vil programmet informere deg om din anti-virusdatabase er ajour.
3. Størrelsen på oppdatering feltet viser hvor størrelsen på oppdateringen. Dersom det ikke er behov for oppdatering vil prosessen avsluttes. Dersom det finnes nyere oppdateringer på serveren, vil nedlastingen starte. Du kan følge med på prosessen i vinduet **Oppdaterer anti-virusdatabasen**. **Totalt nedlastet** forteller deg hvor mye som er lastet ned i den økten. Når nedlastingen er ferdig, vil programmet automatisk oppdatere anti-virusdatabasen og eventuell applikasjonsmodulene



Bilde 19. Oppdaterer anti-virusdatabasen.

---

# KAPITTEL 13. UTVIDEDE INNSTILLINGER

Kaspersky Anti-Virus tilbyr flere framgangsmåter for å konfigurere og tilpasse produktet;

- Avanserte alternativer for sanntidssøk og Avanserte alternativer for skanning
- Objekter i karantene
- Behandle rapporter
- Utvidede innstillinger.

Dette kapittelet inneholder detaljert beskrivelse av de nevnte mulighetene.

## 13.1. Avanserte alternativer for sanntidssøk

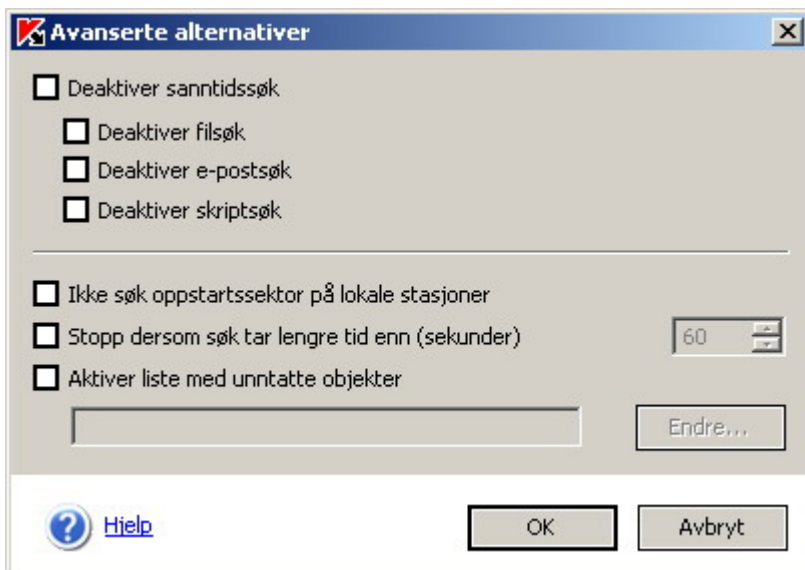
Som standard er Kaspersky Anti-Virus konfigurert til å bruke anbefalte innstillinger på sanntidssøk fra Kaspersky Lab, men du kan selv konfigurere disse innstillingene dersom det er ønskelig. Ved å konfigurere sanntidssøk kan du velge å utelate objekter som skal skannes ved sanntidssøk.



Generelle skanneparametere kan også konfigureres ved å velge beskyttelsesnivå (**Maksimal beskyttelse**, **Anbefalt nivå**, **Høy hastighet**).

For å få tilgang konfigurasjonen, klikk Avanserte alternativer i **Innstillinger for sanntidssøk** vinduet (se Bilde 14). Du kan velge at sanntidssbeskyttelsen ikke skal søke i **filer**, **e-post** og **skript**. Du kan også velge om Kaspersky Anti-Virus ikke skal skanne **oppstartssektor** på lokale stasjoner, og hvor lenge et objekt skal analyseres før programmet går videre til neste objekt.

Her kan du velge å utelate objekter fra skanningen ved å markere alternativet. Du kan også velge å utelate filformater ved å markere  **Aktiver liste med unntatte objekter**, og klikke **Endre**. Definer de utelatte objektene ved å spesifisere plassering eller filter (for eksempel \*.bmp).



Bilde 20. Avanserte alternativer for sanntidssøk

Eksempler på filter som kan utelates. "?" kan representere hvilken som helst bokstav:

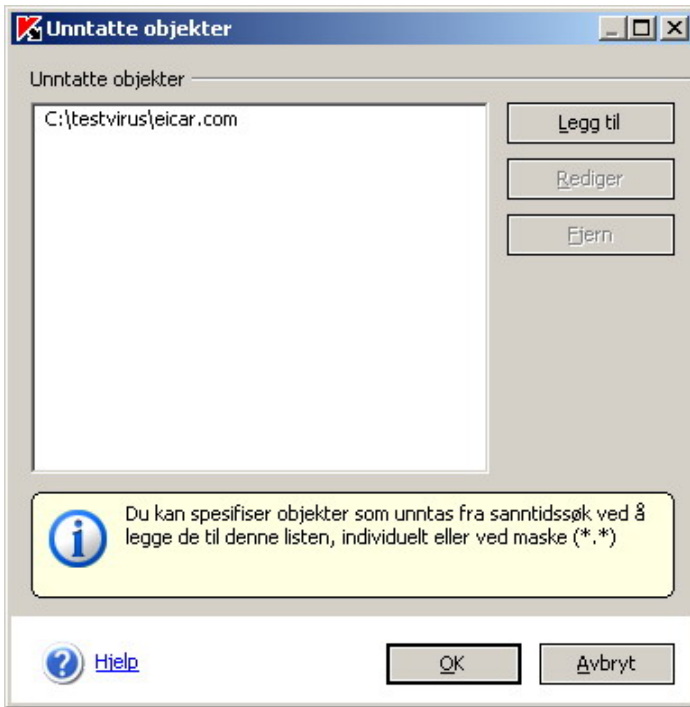
- Filter uten å spesifisere plassering:
  - **\*.exe** - alle filer med endelsen exe
  - **\*.ex?** - alle filer med endelsen ex?
  - **test** - alle filer med filnavnet test
- Filter med spesifisert plassering:
  - **C:\dir\\*.\*** - alle filer i mappen C:\dir\
  - **C:\dir\\*.exe** - alle filer med endelsen exe i mappen C:\dir\
  - **C:\dir\\*.ex?** - alle filer med endelsen ex? i mappen C:\dir\
  - **C:\dir\test** - bare filen C:\dir\test
  - **C:\dir\** - alle filer i mappen C:\dir\ og dens undermapper
- Filter i henhold til plassering:
  - **dir\\*.\*** - alle filer i alle undermapper av dir\
  - **dir\test** - alle filer med filnavn test i undermapper av dir\

- **dir\\*.exe** - alle filer med endelsen exe i alle undermapper av dir\
- **dir\\*.ex?** - alle filer med endelsen ex? i alle undermapper av dir\
- **dir\** - alle filer i alle mapper under dir\ og undermapper



Filter \*.\* og \* er ikke mulig hvis ikke plassering er spesifisert.

I vinduet **Unntatte objekter** (se Bilde 21) kan du forandre listen over objekter som unntas ved sanntidssøk ved å velge **Legg til**, **Rediger** eller **Fjern**. Når listen er komplett, klikk **OK**.



Bilde 21. Spesifiser unntatte objekter i sanntidssøk

Dersom du velger gjenopprette anbefalte innstillinger, vil du forkaste alle innstillingene du har forandret.

For å gjenopprette standard innstillinger for sanntidssøk, klikk gjenopprette anbefalte innstillinger på høyremenyen i **Innstillinger** arkfanen (se Bilde 22).

**Anbefalt nivå for sanntidssøk er i bruk.**

Ved oppdagelse av virus, blokker tilgang og spør om alternativer.

Beskyttelse: Anbefalt nivå.

Du kan [endre innstillinger for sanntidssøk](#).

Bilde 22. Informasjon om sanntidssøk innstillingene.

## 13.2. Avanserte alternativer for skanning

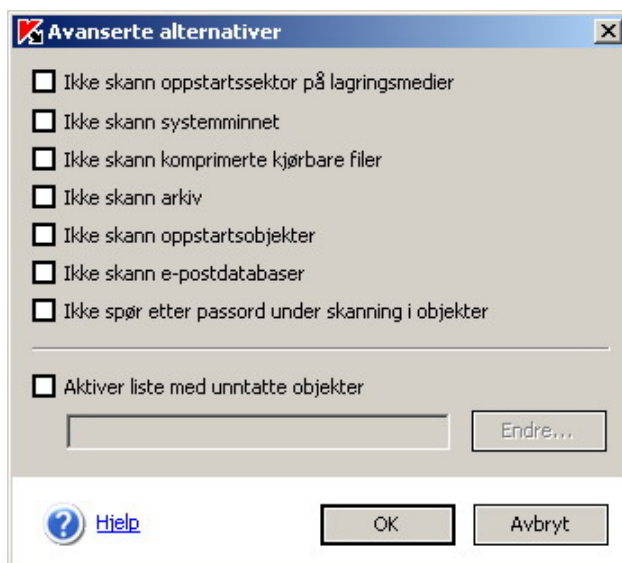
Som standard skanner Kaspersky Anti-Virus din datamaskin i henhold til disse anbefalte innstillingene fra [Kaspersky Lab](#).

Du kan også forandre disse innstillingene ved å klikke på [Avanserte Alternativer](#) under **Innstillinger for skanning**. De samme avanserte alternativene finner du under **Innstillinger for sanntidssøk**




Generelle skanneparametere kan også konfigureres ved å velge beskyttelsesnivå (**Maksimal beskyttelse**, **Anbefalt nivå**, **Høy hastighet**).

Under Avanserte alternativer kan du velge følgende:



Bilde 23. Spesifiser hva du vil utelate fra skanningen.

Her kan du velge å utelate objekter fra skanningen ved å markere alternativet. Du kan også velge å utelate filformater ved å markere  **Aktiver liste med unntatte objekter**, og klikke **Endre**. Definer de utelatte objektene ved å spesifisere plassering eller maske (for eksempel \*.bmp).



Det anbefales at du ikke utelater logiske diskene ved å bruke *subst* kommandoen. Kaspersky Anti-Virus gjenkjenner disse som mapper og vil derfor skanne de.

For å gjenopprette de anbefalte innstillingene, klikk [gjenoppsett standardinnstillinger](#) på høyremenyen under **Innstillinger** arkfanen.

## 13.3. Behandle objekter i karantene

Heuristisk analyse oppdager ca 92% av nye forekomster av ondsinnet kode. Slik funksjonalitet er meget effektiv, men kan av og til gi falsk deteksjon av virus. Er det mulig å bekrefte om et objekt faktisk er infisert med et nytt virus eller om det bare er en falsk alarm?

Under skanningen av din datamaskin eller andre objekter i sanntid, vil Kaspersky Anti-Virus plassere alle mistenkelige objekter i karantene. Du kan senere velge hva som skal gjøres med disse objektene. Karantenen er egentlig en spesialfil som lagrer alle disse objektene hvor de ikke kan skade din datamaskin.

Du bør oppdatere din anti-virusdatabase før du kjører en skann på karantenen. Nyere anti-virusdatabase kan inneholde informasjon om disse mistenkelig infiserte objektene, og du kan dermed forsøke å reparere de.

Du kan selv håndtere objektene som er plassert i **karantene** ved å klikke på Vis karantene i venstremenyen på Beskyttelse arkfanen.

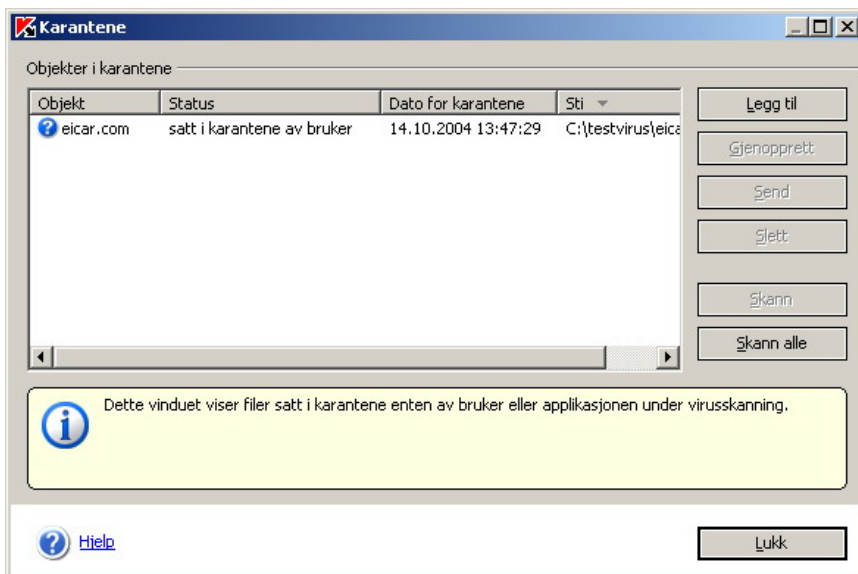
I **Karantene** vinduet kan du gjøre følgende:

- plassere et mistenkelig objekt i karantene. Klikk **Legg til** og velg filen du ønsker å legge i karantene.
- **Skann** eller **Skann alle** objektene i karantene. Det er viktig at du oppdaterer anti-virusdatabase.

Etter skanning av objektene blir status forandret til *infisert*, *falsk alarm*, ikke *infisert* m.v. Programmet vil så gi anbefalinger om hva som bør foretas med objektet.

*Infisert* status betyr at objektet er infisert, men programmet kan ikke rense filen. Det anbefales å slette slike objekter.

Alle objekter med status *falsk alarm* kan bli gjenopprettet. Disse objektene er ikke infiserte



Bilde 24. Karantene for mistenkelige objekter

- Objekter som gjenoprettes vil bli flyttet til objektets originale plassering. For å gjenopprette et objekt, marker objektet i listen og klikk **Gjenopprett**. For å gjenopprette objekter fra sammensatte filer, e-post databaser og lignende, må du spesifiserer hvor du ønsker objektet plassert..



Det anbefales å bare gjenopprette objekter som har status *falsk alarm, ikke infisert, renset!*

- Sende mistenkelige objekter til Kaspersky Lab for analyse. Det anbefales bare å sende de objektene som har status *mulig infisert* etter gjentatte forsøk på å rense objektet med de nyeste anti-virusdatabaser. For å sende et slikt objekt, klikk Send (se seksjon Kontakte brukerstøtte).



Husk at du må oppdatere anti-virusdatabasen din og skanne objektet før du sender det til Kaspersky Lab.

- Slette et objekt eller en gruppe objekter fra karantenen. Det anbefales bare å slette filer som ikke kan renses. Marker filene du ønsker å slett, og klikk **Slett**.

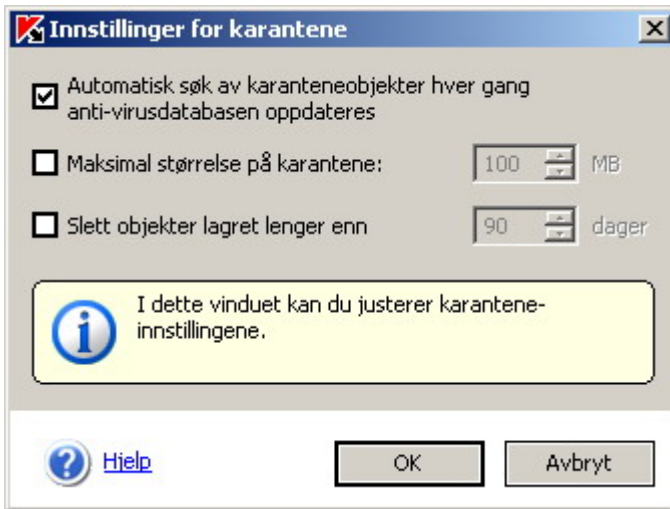
## 13.4. Innstillinger for karantene

Du kan endre innstillingene for karantenen ved å klikke [Innstilling for karantene](#) (se Bilde 25) i venstre menyen på **Innstillinger** arkfanen:

- ✓ **Automatisk søk av karanteneobjekter hver gang anti-virusdatabasen oppdateres.** Denne funksjonen starter en automatisk skann av alle objektene i karantene hver gang anti-virusdatabasen blir oppdatert.



Dersom du arbeider med karanteneobjektene kan ikke Kaspersky Anti-Virus starte en automatisk skann.



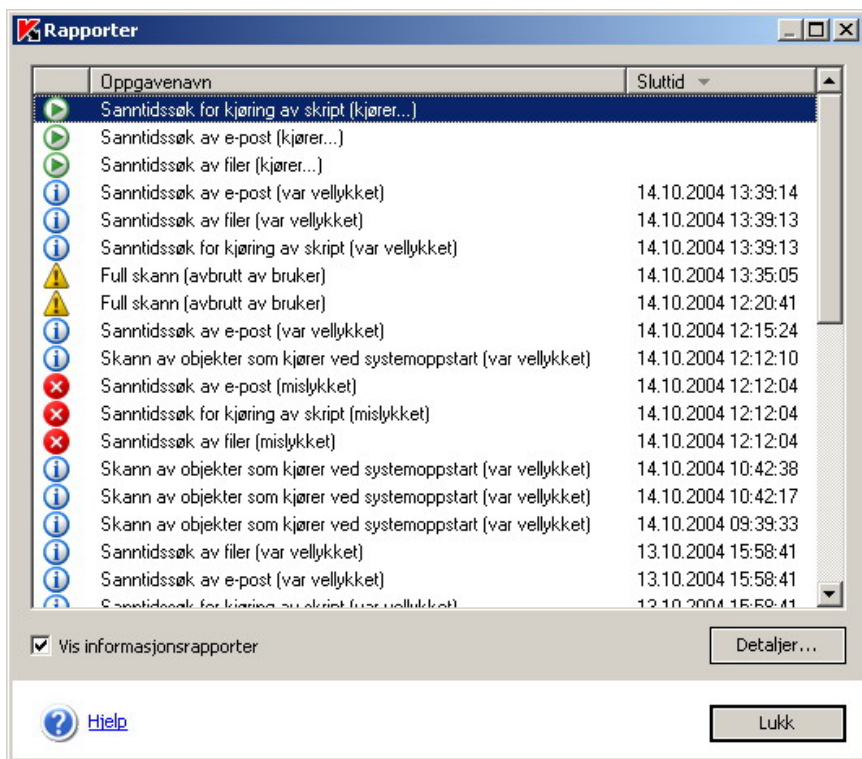
Bilde 25. Innstillinger for karantene

- ✓ **Maksimal størrelse på karantene:** Som standard er denne størrelsen ikke definert. Det vil si alle objekter som plasseres i karantene blir der til du manuelt fjerner dem. Dersom du ønsker å definere maksimal størrelse på karantenen, kan du markere [Maksimal størrelse på karantene](#) og definere størrelsen i tekstfeltet (standard er 100 MB).
- ✓ **Slett objekter lagret lengre enn.** Som standard er lagringstiden på objektene i karantene ikke begrenset. Du kan forandre denne innstillingen ved å markere [Slett objekter lagret lengre enn](#), og definere antall dager i tekstfeltet (standard er 90 dager).

## 13.5. Behandle rapporter

Programmet samler rapporter under skanning, oppdatering og under sanntidssøk. Rapportene inneholder informasjon om skannede objekter, behandlingsresultat og generell statistikk.

En komplett liste over alle oppgaver som utføres eller er utført av Kaspersky Anti-Virus er tilgjengelig fra **Rapportvinduet** (se Bilde 26). Du åpner vinduet ved å klikke Vis rapporter fra venstre menyseksjon i **Beskyttelse** arkanen i hovedvinduet. Status for hver oppgave, og dato/klokkeslett for slutførelse av oppgaven lagres i rapportene.





Bilde 26. Rapporter

Status for rapporten angis med følgende ikoner:

 eller  – *Informasjonsrapporter* (for eksempel, oppgave startet, oppgave fullført, oppgave under utførelse, oppgave er på vent)

 – *Advarsel* (for eksempel, Advarsel! Infisert objekt er ikke behandlet.

 – *Notis* (for eksempel, oppgaven er avbrutt).

Informasjonsrapporten vises som referanse, og er ikke av spesiell interesse. Du kan skru av visning av disse meldingene ved å fjerne markeringen i boksen  **Vis informasjonsrapporter**.

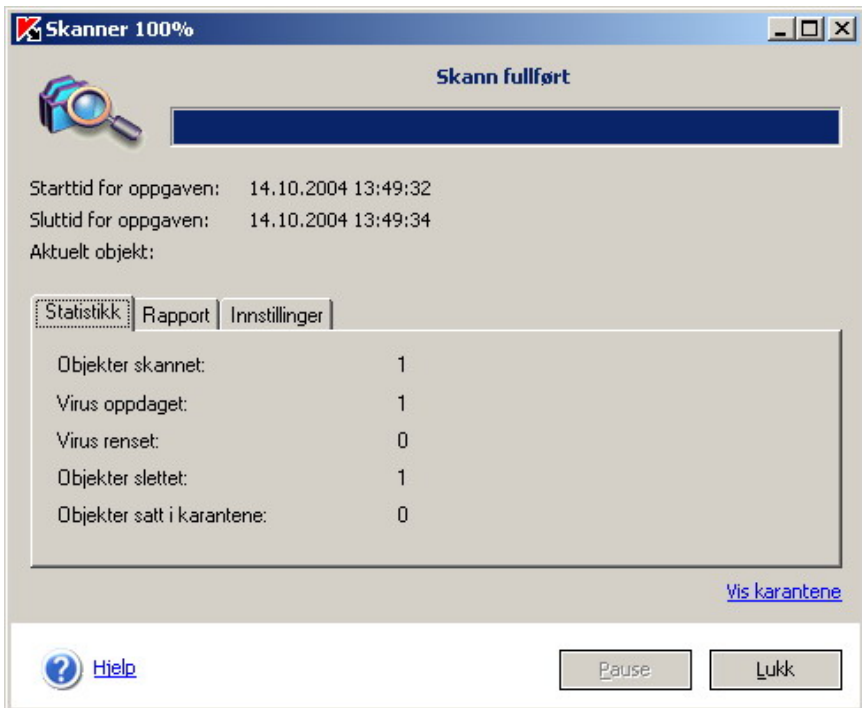
Du kan også sortere rapporter på type, tittel - eller ved klokkeslett. For å gjøre dette klikker du på overskriften for kolonnen du ønsker som sorteringsrekkefølge.

Du kan se innstillinger for hver enkelt oppgave i loggfilen, statistiske data og resultater ved å klikke **Detaljer** eller dobbeltklikke oppgaven..

Dette åpner ett nytt vindu, med en detaljert rapport om oppgaven ved hjelp av arkfanene **Statistikk**, **Rapport** og **Innstillinger**




Under en full skanning, kan du på denne måten overvåke oppgavens ytelse.



**Skanner 100%** \_ □ ×

**Skann fullført**




Starttid for oppgaven: 14.10.2004 13:49:32  
 Sluttid for oppgaven: 14.10.2004 13:49:34  
 Aktuelt objekt:

**Statistikk** | Rapport | Innstillinger

Objekter skannet:	1
Virus oppdaget:	1
Virus renset:	0
Objekter slettet:	1
Objekter satt i karantene:	0

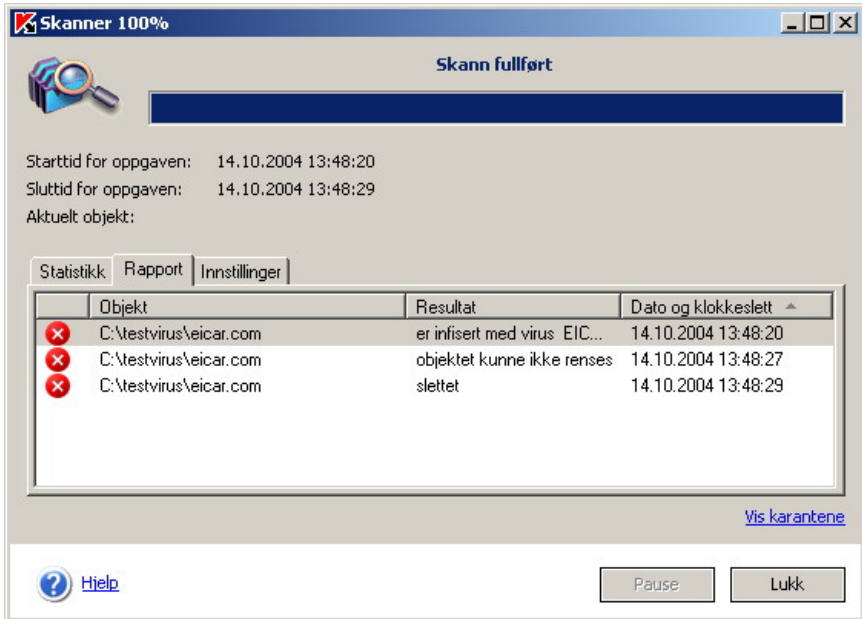
[Vis karantene](#)

 [Hjelp](#) Pause Lukk

Bilde 27. Statistikk arkfanen

For sanntidssøk og skanning:

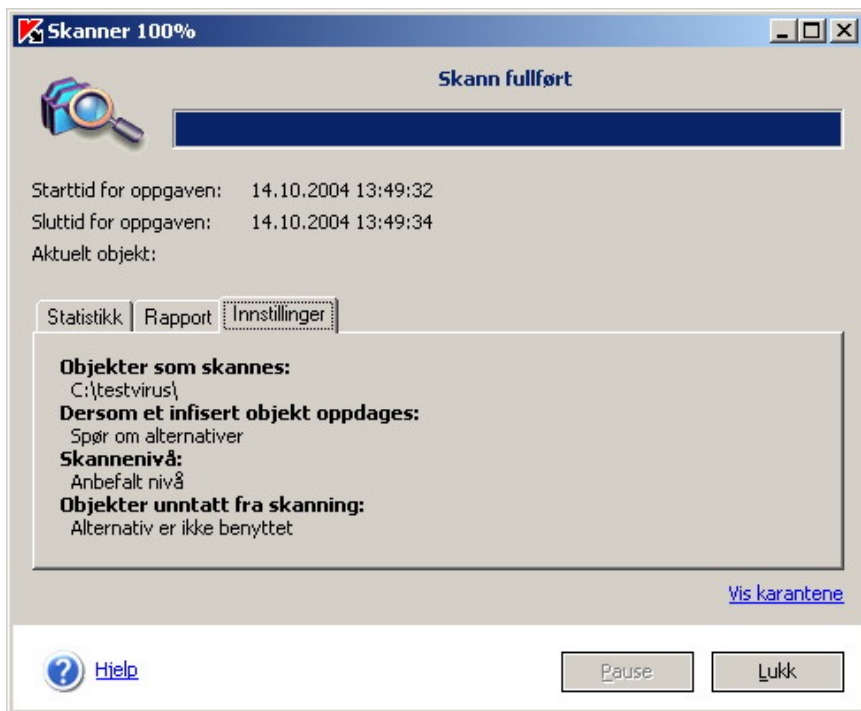
- **Statistikk** inkluderer generell informasjon om utførte elementer innefor rammen til oppgaven: dato og klokkeslett for oppgave-start og slutt, totalt antall filer som skannes, også informasjon om infiserte, slettede, rensede objekter og objekter satt i karantene.
- **Rapport** inneholder ingen informasjon om virusfrie objekter - og viser kun informasjon om oppdagede virus. For å vise informasjonen, marker  **Lagre alle meldinger** i vinduet **Utvidede innstillinger**. Dersom dette er valgt vil **Rapport** inneholde detaljert informasjon om hvert objekt som er skannet. Du kan også velge visning av informasjonsmeldinger i denne arkfane. Dersom du ikke vil vise informasjonsmeldinger, kan du åpne hurtigmenyen ved å dobbelklikke **Rapport** arkfane og avmarkere  **Vis detaljert rapport**.
- Når du leser rapporter mens skanning pågår, vil du som standard alltid se nyeste post i loggen. For å skru av dette alternativet, kan du åpne hurtigmenyen ved å høyreklikke i vinduet og avmarkere  **Vis nyeste innhold i rapporten** eller velge en post i rapporten.
- **Innstillinger** viser hvilke innstillinger oppgaven benyttet - inkludert nivå for skanning og handlingsalternativer for oppdagelse av infiserte objekter, skadelig kode og mulig infiserte objekter. Denne informasjonen inkluderer også unntaksliste, dersom disse er spesifisert.



Bilde 28. Rapport arkfanen

Følgende informasjon relatert til oppdatering av anti-virusdatabasen og applikasjonsmoduler vises:

- **Statistikk** inkluderer generell informasjon om utførte elementer innenfor rammen til oppgaven: dato og klokkeslett for oppgave-start og slutt, totalstørrelse av oppdatering på oppdateringskilden (Kaspersky Labs servere eller lokal mappe), og størrelse på oppdatering som er lastet ned til din datamaskin.
- **Rapport** inkluderer informasjon om hvert element i prosessen: etablering av forbindelse mot oppdateringsservere, nedlastede filer og installasjonsinformasjon. Denne informasjonen vises alltid uavhengig om  **Lagre alle meldinger** i **Utvidede Innstillinger** er markert.
- **Innstillinger** viser hvilke innstillinger oppgaven benyttet - inkludert oppdateringsinnstillinger, oppdateringstype og fra hvilken kilde oppdateringene ble nedlastet.



Bilde 29. Innstillinger arkanen

Du kan også velge hvilken oppgave du ønsker å se på i **Rapportvinduet** eller i en detaljert dialogboks ved hjelp av **Neste** > og < **Forrige** knappene, eller ved å velge navnet på oppgaven fra nedtrekksmenyen.

### 13.5.1. Se informasjon i rapporter

Kaspersky Anti-Virus gir deg muligheten til selv å velge hva rapportene skal inneholde. Dersom du ønsker det kan rapportene bare inneholde viktig informasjon, mens informative og andre refererende meldinger ikke blir lagret.

Dersom du ønsker å lagre alle informasjonsmeldinger i rapportene, marker  **Lagre alle meldinger** i **Utvidede innstillinger**. Du kan se alle meldingene som Kaspersky Anti-Virus genererer i **Skannvinduet** når du skanner din datamaskin.

Hvis du har markert Logg alle meldinger, vil alle informasjonsmeldinger blir lagret i rapporten.

Hvis du ikke har markert **Logg alle meldinger**, vil rapporten bare inneholde viktige informasjonsmeldinger (for eksempel om et objekt ikke har blitt skannet på grunn av feil).



For å ikke å vise detaljerte meldinger under skanningen:

høyre-klikk i Rapport fanen for å åpne en hurtigmeny, og klikk **Vis detaljert rapport**



Bilde 30. Hurtigmenyen – Rapport arkfanen



Hvis  **Logg alle meldinger** i **Utvidede innstillinger** ikke er markert, vil **Vis detaljert rapport** ikke være tilgjengelig!

Når du overvåker rapporten i sanntid (for eksempel mens du skanner din datamaskin), vil du som standard se det nyeste innholdet i rapporten. Dersom du ønsker å skru av dette kan du klikke på  **Vis nyeste innhold i rapporten** i samme hurtigmeny, eller bare klikke på en av oppgavene i rapporten.

## 13.5.2. Eksportere og sende rapporter

**Behandle Rapporter** gir deg mulighet til å eksportere og sende rapporter fra Kaspersky Anti-Virus. Du har tilgang på flere alternativer ved å høyre-klikke på en av rapportene i listen.



Bilde 31. Hurtigmeny for å behandler rapporter

De forskjellige rapportene har forskjellige alternativer; Send rapport til Kaspersky Lab er bare tilgjengelig for rapporter av typen **Advarsel** (for eksempel hvis programmet har rapportert en programfeil). Merk også at du ikke kan slette en rapport dersom oppgaven kjører (beskrivelsen av rapporten slutter med "(kjører...)").

Eksportere en detaljert rapport til fil produserer en fil hvor innholdet er tilgjengelig i en Microsoft Excel tabell.

Hvis en oppgave (for eksempel anti-virusdatabasen oppdateres) blir avbrutt eller feiler av en ukjent årsak, kan du sende rapporten til Kaspersky Lab for undersøkelse.

For å gjøre dette, høyre-klikk på rapporten i **Behandle Rapporter** vinduet, og velg Send rapport til Kaspersky Lab. Dette vil åpne en e-post fra din standard e-postklient med rapporten vedlagt. Send denne e-posten til Kaspersky Lab for undersøkelse.



E-post meldinger er automatisk generert dersom du benytter Microsoft Outlook eller Microsoft Outlook Express som din e-postklient. Dersom du benytter andre e-postklienter må du først konfigurere programmet til å støtte Simple MAPI.

## 13.6. Utvidede innstillinger

Utvidede Innstillinger finner du under **Innstillinger** arkfanen. Her kan du konfigurere de følgende oppgavene:

- Vis varslingsmeldinger** - tillate programmet å bruke varslingsmeldinger for å informere brukeren om oppgaver. Det anbefales ikke å skru av denne funksjonaliteten fordi varslingsmeldingene ofte ber brukeren om å foreta et valg.
- Bruk varslingslyder** - tillate programmet å bruke varslingslyder for å informere brukeren om hendelser. Hvilke lydfilene som benyttes kan forandres i **Start→Kontroll Panelet→ Lyder og lydenheter→Lyder**.
- Lagre alle meldinger** - skru på lagring av alle meldinger som blir generert av programmet i rapportene (informasjonsmeldinger, feilmeldinger m.v). Som standard inneholder rapportene bare viktige meldinger, slik som kritiske feil, oppgavefeil, avbrutte oppgaver m.v)
- Ikke lagre meldinger lengre enn** - alle rapporter lagret i 30 dager (standard). Du kan forandre denne lagringsperioden ved å forandre antall dager i roteringsmenyen, eller ved å fjerne lagring av rapporter (huk av merket i avkrysningsboksen). Ved programoppstart vil rapporter som er eldre enn angitt lagringstid bli fjernet.
- Start Kaspersky Anti-Virus Personal ved oppstart** - skru på automatisk oppstart av Kaspersky Anti-Virus Personal ved oppstart av din datamaskin. Dersom du ikke markerer dette alternativet, vil Kaspersky Anti-Virus Personal ikke starte neste gang du starter din datamaskin, og anti-virusfunksjonene vil ikke være tilgjengelige.



Det anbefales ikke å skur at automatisk oppstart av Kaspersky Anti-Virus da dette kan føre til infeksjon av din datamaskin.

Du kan ikke forandre denne innstillingen dersom du ikke har administrative rettigheter på denne datamaskinen



**Bruk passord for å beskytte applikasjonen** - skru på bruk av passordbeskyttelse ved forandring av programinnstillinger. Vi anbefaler at du benytter passordbeskyttelse dersom det finnes andre brukere av denne datamaskinen, og du ikke vil at de skal kunne forandre innstillinger i Kaspersky Anti-Virus Personal, skru av beskyttelsen eller benytte programmet til andre hensikter. Etter du har skrudd på denne funksjonen, skriv inn ditt passord i **Passord** feltet, og gjenta det samme passordet i **Bekreft passord**.

**Utvidede innstillinger**

Grensesnitt

- Vis varslingsmeldinger
- Bruk varslingslyder

Rapporter

- Lagre alle meldinger
- Ikke lagre rapporter eldre enn  dager

Start

- Start Kaspersky Anti-Virus Personal ved oppstart

Beskyttelse

- Bruk passord for å beskytte applikasjonen

Passord:

Bekreft passord:

[Hjelp](#)

Bilde 32. Utvidede innstillinger for Kaspersky Anti-Virus Personal.

---

# APPENDIX A. KONTAKTE BRUKERSTØTTE

Kaspersky Labs brukerstøtte er tilgjengelig for alle brukere av Kaspersky Anti-Virus med gyldig lisensnøkkel. Ta kontakt med brukerstøtte dersom:

- programmet ikke fungerer normalt, og feilmeldinger forekommer ofte.
- dersom Kaspersky Anti-Virus oppdager et mulig infisert objekt som inneholder kritiske data og blokkerer tilgang til objektet, men du trenger å arbeide med objektet.



*For å sende en melding til Kaspersky Lab's brukerstøtte:*

klikk Send spørsmål til brukerstøtte i venstremenyen under **Brukerstøtte** arkfanen.

Programmet vil automatisk lage en ny e-post melding i ditt standard e-postprogram, for eksempel Microsoft Outlook. Inneholdet i e-posten er allerede fylt ut med nødvendig informasjon som brukerstøtte trenger for å kunne bistå deg. Før du sender e-posten, skriv en detaljert forklaring på problemet. Våre konsulenter på brukerstøtte vil forsøke å svare på din henvendelse så snart som mulig.

Hvis Kaspersky Anti-Virus plasserer et mulig infisert objekt i karantene, bør du oppdaterer anti-virusdatabasen og forsøke å rense objektene en gang til (se seksjon **Objekter i karantene**). Dersom programmet ikke kan rense det mistenkelige objektet, kan du sende objektet til Kaspersky Lab brukerstøtte for analyse. Objektet kan være infisert med et ukjent virus, eller det kan være en falsk alarm



**Advarsel! Dersom du ønsker å sende mistenkelige filer til Kaspersky Lab må du først skanne objektene med de nyeste anti-virusdatabasen. Anti-virusdatabasen må være fra den samme dagen du sender objektet!**



*For å sende et objekt til Kaspersky Lab for analyse:*

marker filen fra listen i **Karantene**, og klikk Send.

Programmet vil automatisk lage en e-post melding i ditt standard e-postprogram, for eksempel Microsoft Outlook, med den mistenkelige filen som vedlegg. Dersom du sender denne e-posten, vil eksperter fra Kaspersky Lab analysere

filen og forsøke å gjenskape data dersom dette har blitt tapt. Etter ekspertene er ferdig med analysen vil du motta en detaljert tilbakemelding.



Husk at hver fil du sender må ha blitt skannet av Kaspersky Anti-Virus minst en dag før du sender den.

Dersom du mener en eller flere filer på din datamaskin er infisert, men Kaspersky Anti-Virus ikke oppdager det, kan du fortsatt sende filen til analyse hos Kaspersky Lab.



*For å sende filer du mistenker for å være infiserte til Kaspersky Lab:*

klikk Send fil til analyse i venstremenyen under **Brukerstøtte** arkfanen. Legg ved de mistenkelige filene.

For å sende en fil til Kaspersky Lab, følg de samme framgangsmåten som om du skulle sende et objekt fra **Karantene** vinduet.

---

# APPENDIX B. ORDLISTE

I denne hjelpefilen vil du møte uttrykk som er spesifikke for anti-virusbeskyttelse. Formålet med denne ordlisten er å gi deg en forklaring på de forskjellige uttrykkene. Innholdet er alfabetsortert, for å forenkle søkeprosessen.

## A

**Anbefalt nivå** - Det optimale nivået med beskyttelse som er anbefalt av Kaspersky Lab. Som standard er beskyttelsesnivået satt til Anbefalt nivå.

**Anti-virusdatabase** - En database laget av Kaspersky Lab som inneholder detaljert informasjon om alle eksisterende virus og metoder for å oppdage og rense disse. Vår sentrale database oppdateres regelmessig (hver time) med informasjon om nye virus - så fort disse oppdages - for å holde din datamaskin konstant beskyttet mot virus. Du trenger derfor å oppdatere din anti-virusdatabase så ofte som mulig, helst hver tredje time.

**Anti-virus beskyttelsestatus** - Nåværende status for antivirsbeskyttelsen som karakteriserer sikkerhetsnivået på din datamaskin.

**Arkiver**- Filer som inneholder en eller flere filer, som kan være arkiver

## E

**E-postdatabase** - En database som inneholder e-postmeldinger. All e-post (både innkommende og utgående) lagres i databasen etter at sending/mottak er utført. Disse databasene gjennomføres når du velger å skanne hele datamaskinen. Kaspersky Anti-Virus sanntidssøk skanner all innkommende og utgående e-post før de sendes eller mottas.

## F

**Falsk alarm** - Tilfeller der en uidentifisert applikasjon markeres som infisert fordi den inneholder kode som ligner virus.

**Falske positive** - se falsk alarm.

**Forebyggelse** - Sikkerhetsmekanismer som hindrer viruspenetrasjon på din datamaskin. Eksempler på slike mekanismer er omfattende virusbeskyttelse og tilgang til oppdaterte versjoner av dine applikasjoner

## H

**Heuristisk kodeanalyse** - En meget effektiv teknologi som lar applikasjonen oppdage ukjente virus. Teknologien oppdager objekter som er infisert med ukjente virus samt nye varianter av kjente virus.

**Høy hastighet** - Et beskyttelsesnivå som begrenser skanningen til objekt typer som kan infiseres. Dette reduserer skannetiden betraktelig.

**Hoppe over** - Behandlingsmetode hvor tilgang til objektet nektes (gjelder bare sanntidsbeskyttelse), og informasjon om objektet loggføres i applikasjonsrapporten, men ingen andre handlinger utføres

## I

**Infisert objekt**- Et objekt som inneholder virus. Det anbefales at du ikke åpner slike objekter fordi det kan medføre at datamaskinen infiseres. Dersom et *infisert* objekt oppdages, bør du forsøke å *rense* objektet med Kaspersky Anti-Virus, eller slette objektet dersom rensing ikke er.

## K

**Karantene** - En mappe hvor Kaspersky Anti-Virus plasserer alle *mulig infiserte objekter*. Objektene blir ufarlige for din datamaskin så lenge de er plassert i denne datamaskinen.

**Karantene (sette objekt i karantene)** - En metode for å behandle *infiserte* eller *mulig infiserbare* objekter ved å blokkere tilgang på objektet og plassere det i karantene mappen for videre behandling.

**Kaspersky Anti-Virus moduler**- Kaspersky Anti-Virus Personal består av flere programmoduler. Hver av disse modulene utgjør en spesifikk funksjon i Kaspersky Anti-Virus, for eksempel *sanntidssøk*, *manuell skanning*, *oppdatering* m.v.

**Kaspersky Labs oppdateringsservere** - En liste over http- og ftp-servere som Kaspersky Lab bruker for å utgi oppdateringer til anti-virusdatabaser og applikasjonsmoduler..

**Kun rapport** - Når *infiserte* eller *mistenkelige objekter* oppdages (i sanntidssøk), vil programmet blokkere objektet og rapportere oppdagelsen

## L

**Lisensnøkkel** - En fil med ekstensjonen ".key", som er din personlige nøkkel. Lisensnøkkel følger med som en del av pakken, dersom du kjøpte en kopi av Kaspersky Anti-Virus fra en Kaspersky Lab forhandler. Dersom du har kjøpt produktet via netthandel, vil lisensnøkkel sendes til deg per e-post.Kaspersky Anti-Virus Personal VIRKER IKKE uten lisensnøkkel.

**Lisensperiode** - En periode, hvor du i hele perioden kan bruke Kaspersky Anti-Virus. Lisensperioden defineres av en gyldig lisensnøkkel, og normalt ett år frem i tid etter første installasjon av nøkkelen. Når lisensen løper ut (ikke er gyldig) vil programmet fremdeles fungere, men du vil ikke kunne oppdatere anti-virusdatabasen

**M**

**Maksimal beskyttelse** - Ett beskyttelsesnivå som sikrer maksimal beskyttelse mulig for Kaspersky Anti-Virus Personal. Med dette nivået aktivert, vil alle filer lagret på din datamaskin, flyttbare medier og nettverksstasjoner (dersom de er koblet til din datamaskin) skannes for virus.

**Malware** - ett ord som en er sammentrekning av "malicious software" ("skadelig programvare") og er en generisk terminologi for virus, trojaner og ormer.

**Minne** - Mengden RAM installert på din datamaskin.

**Mulig infiserte objekt**- Att objekt som inneholder kode fra et ukjent virus eller en kode som minner om et kjent virus. Mulig infiserbare objekter oppdages av den *heuristiske kodeanalysen*

**O**

**Objekter som kjøres ved oppstart** - Ett sett med programmer som kreves for å starte korrekte funksjon av operativsystemet på din datamaskin. Ditt operativsystem kjører disse objektene ved hver oppstart. Noen virus infiserer *oppstartsobjekter*, og kan dermed hindre start av operativsystemet.

**OLE-objekt** - Ett objekt lenket eller innebygd i en annen fil. Kaspersky Anti-Virus skanner slike objekter for virus. For eksempel kan ett Microsoft Excel regneark innebygges i ett Microsoft Word dokument, og vil da skannes av Kaspersky Anti-Virus som ett OLE-objekt.

**Oppdatering av anti-virusdatabasen** - En funksjon i Kaspersky Anti-Virus som vedlikeholder gyldigheten av beskyttelses på din datamaskin. Oppdateringsprosessen inkluderer kopiering av *anti-virusdatabasen* fra Kaspersky Labs *oppdateringsservere* til din datamaskin, og en automatisk integrasjon med databasen i Kaspersky Anti-Virus Personal.

**Oppstartsektor** - Ett bestemt område på harddisken som inneholder operativsystemets referanse til last av programmet.

**Oppstartsektor** - Ett område på harddisken eller ett flyttbart medie (for eksempel, en diskett eller en CD-ROM). Det finnes oppstartsvirus som infiserer *oppstartssektorer*. Kaspersky Anti-Virus skanner begge sektorer for virus og sletter virus dersom en infeksjon oppdages.

**Oppstartsvirus** - Ett virus som infiserer *oppstartssektoren* på dine harddisker og operativsystemet som er installert på din datamaskin. Under en systemoppstart vir viruset tvinge systemet til å laste viruset i minnet og så overgi kontroll fra den originale lastekoden til virusets kode

**P**

**Pakkede filer** - Filer som inneholder programmer og instruksjoner til operativsystemet for kjøring av programmet.

**Potensielt infiserbart objekt** - Ett objekt som kan infiseres. Potensielt infiserbare objekter er som regel kjørbare filer, som for eksempel filer med .com, .exe og tilsvarende ekstensjoner

**Q**

**Quarantine** – A folder to which Kaspersky Anti-Virus® moves all *possibly infected objects* found during either a *full scan of your computer* or in *real-time protection mode*.

**Quarantining (moving to the quarantine folder)** – A method of treating an *infected* or *possibly infected object* by denying normal access to the object and moving it to the quarantine folder for subsequent treatment.

**R**

**Rense** - En metode for behandling av infiserte objekter. Rensing kan resultere i delvis eller komplett fjerning av skadelig kode fra infiserte data, eller en avgjørelse at disse filene ikke kan renses. Objekter renses ved hjelp av poster (metoder) i anti-virusdatabasen.

**S**

**Sanntidssøk** -En funksjon i Kaspersky Anti-Virus som startes automatisk når systemet starter opp - hvor alle objekter skannes for virus når de åpnes, lagres eller kjøres. Dersom et objekt blir identifisert som infisert eller misstenkelig, vil Kaspersky Anti-Virus blokkere tilgangen og forsøke å behandle det (rense, sette i karantene, slette etc.) eller varsle brukeren om mulige handlingsalternativer.

**Sikkerhetskopi (utføre)** - Lager en sikkerhetskopi av filen i mappen BACKUP før den behandles (renses eller slettes). Filen kan siden gjenopprettes fra sikkerhetskopien, for eksempel for vider skanning med ny versjon av anti-virusdatabasen.

**SIKKERHETSKOPI** - En mappe som inneholder sikkerhetskopier av slettede og rensede objekter

**Skanning** -En funksjon av programmet som startes av brukeren (eller ved tidsplanlegging) som skanner alle filer av alle typer på din datamaskin.

**Skript** - En programfil som inneholder en sekvens med handlinger som for eksempel kan være innebygd i en nettside og kjøres av nettleseren (som Microsoft Internet Explorer), eller det kan være frittstående filer som kjøres av Windows operativsystemet. I sanntidssøk overvåker Kaspersky Anti-Virus kjøring av skript, stopper de og skanner det for virus. Avhengig av skannerresultatet kan du for eksempel tillate eller blokkere kjøring av skriptet.

**Slette et objekt**- En metode for behandling av et objekt. Å slette et objekt betyr å fjerne det fysisk fra din datamaskin. Denne metoden er anbefalt for objekter som ikke kan renses.

**Sti** - Et sted hvor en samling filer for oppdatering ligger. Oppdateringer lastes ned via Internett og installeres på din datamaskin

## U

**Ukjent virus** - Ett nytt virus som ikke er registrert i *anti-virusdatabasen*. Kaspersky Anti-Virus oppdager ukjente virus ved å benytte *heuristisk kodeanalyse*, og objekter som inneholder denne type virus merkes som *mulig infisert*.

**Unntatte objekter** - Brukerdefinerte innstillinger som ekskluderer bestemte objekter fra skanningen. Du kan definere egne regler for *sanntidssøk* og for *skanning*. For eksempel kan du utelate arkiver fra skanning ved å bruke ett filter som angir hvilke filer du ikke ønsker skal være med.

---

## APPENDIX C. KASPERSKY LAB

**Kaspersky Labs utvikler, produserer og distribuerer IT-sikkerhetsløsninger som beskytter brukere mot trusler - og gjør det mulig å kontrollere risiko. Kaspersky Labs tilbyr produkter som beskytter data mot virus, hackereangrep og søppelpost (spam) for både hjemmebrukere og bedrifter, og tilbyr konsultasjon og teknisk brukerstøtte**

Historien om Kaspersky Labs begynte i 1989, når Eugene Kaspersky oppdaget et virus på sin datamaskin - og utviklet det første antivirusproduktet under navnet AVP. Selskapet er i dag en internasjonal IT-sikkerhetsleverandør, med hovedkontor i Moskva (Russland) og regionale kontorer i England, Tyskland, Polen, Nederland, Japan, Kina og USA. Selskapets utbredelse er i dag globalt ved hjelp av et partnernetverk på over 500 selskaper.

Kaspersky Labs produkter er sertifisert av West Coast Labs og mottar regelmessig priser fra ledende IT publikasjoner og testlaboratorier. I 2003 oppnådde selskapet "Microsoft Gold Certified Partner"-status for sikkerhetsløsninger. Ekspertene fra Kaspersky Labs er også aktive medlemmer i bransjeorganisasjoner som CARO (Computer Anti-virus Research Organisation) og ICSA (International Computer Security Association).

Kaspersky Labs viruseksperter - med Eugene Kaspersky i spissen - har solid erfaring innen anti-virus bransjen, og forutser med stor nøyaktighet IT-sikkerhetstrender. For eksempel var selskapet først til å introdusere og implementere innovasjoner som heuristisk virusanalyse og lingvistisk tekstanalyse. Slike kontinuerlige innovasjoner holder firmaets produktportefølje fremst i markedet.

Fokusert utvikling over flere år har gjort Kaspersky Labs til en teknologisk leder innen anti-virus. Produktporteføljen inneholder løsninger for å beskytte frittstående datamaskiner, arbeidsstasjoner, filservere, e-post gatewayer, internett gatewayer, brannmurer og håndholdte enheter mot trusler. Kaspersky® Anti-Virus kjernen er integrert i sikkerhetsprodukter fra ledende programvareleverandører som Aladdin, Nokia, ICG, F-Secure, Sybari, G Data, Deerfield, Alt-N, Microworld og Borderware.

I dag er det meste av skadelig kode multifunksjonell og dypt integrert i internettressurser. Tradisjonelle anti-virus løsninger er ikke lenger nok til å beskytte brukere mot eksterne trusler. Kaspersky Labs reagerer pro-aktivt på det til en hver tid skiftende brukerbehovet. Kaspersky Labs har utviklet en personlig brannmur - Kaspersky® Anti-Hacker, så vel som et filter for spam - Kaspersky® Anti-Spam, for å stoppe voksende trusler og for å fullstendig tilfredsstille våre brukeres behov. Som Kaspersky® Anti-Virus, reflekterer disse produktene mange års erfaring og forpliktelse til å beskytte dine data og ditt nettverk.

Kaspersky Labs tilbyr en rekke tjenester for å møte de spesifikke behov for å opprettholde våre brukeres datasikkerhet. Vi lager, tilpasser, implementerer og tilbyr brukerstøtte på sikkerhetsløsninger, og kan også yte konsulentbistand. Vi har databaseoppdateringer hver time, og brukerstøtte hele døgnet på en rekke språk.

## C.1. Andre Kaspersky Lab produkter

### Kaspersky Anti-Virus Personal Pro

Dette programmet er anti-virus beskyttelsen for den erfarne bruker. Omfattende beskyttelse for datamaskiner som kjører Windows 98/ME, Windows 2000/NT, and Windows XP, og med unike beskyttelsesmoduler for MS Office. Løsningen inneholder Office Guard™, som beskytter alle MS Office dokumenter mot makrovirus – samt en kontinuerlig overvåking av alle Visual Basic skript.

Programmet tilbyr en rekke innstillingsmuligheter for alle oppgaver, som for eksempel: full skanning av datamaskinen, oppdatering av anti-virusdatabasen, skann ved kjøring, separat konfigurasjon av individuelle oppgaver og sikkerhetskopi av objekter til egen mappe før objektene renses eller slettes.

Kaspersky Anti-Virus Personal Pro tilbyr:

- **manuell skanning av din datamaskin** - skanner alle lokale lagringsmedier for å oppdage alle former for ondsinnet kode;
- **sanntidsbeskyttelse** - beskytter alle filene dine mot virusangrep;
- **et e-post filter** - skanner alle inn- og utgående e-poster, uten integrering med e-postklienten.
- **kontinuerlig overvåking av skript** - beskyttelse mot makro virus og andre former for skadelig skript.

### Kaspersky Anti-Hacker

Tilkobling til internett medfølger forskjellige typer eksterne farer. Din datamaskin kan bli utsatt for et "hacker"-angrep eller installerte applikasjoner kan forsøke å benytte din internettkobling uten at du er klar over det. Kaspersky® Anti-Hacker er en fullstendig løsning som beskytter din datamaskin mot slike trusler. Programmet stanser alle forsøk på tyveri av informasjon, stanser ondartede programmer som trojanske hester, samt sperrer for uautorisert kommunikasjon.

Kaspersky® Anti-Hacker beskytter applikasjoner mot at utenforstående prøver å bytte ut originale applikasjonsfilene - med en potensielt skadelig versjon. Når ett slikt bytte blir oppdaget, kan du blokkere all videre aktivitet fra denne applikasjonen, eller du kan velge å ikke bry deg om det, dersom du har byttet ut denne applikasjonen selv.

SmartStealth teknologi beskytter deg ved å gjøre din PC 'usynlig'. Når du setter din Anti-Hacker i 'Stealth' modus kan ingen se din PC i nettverket - siden all nettverksaktivitet blir begrenset, dersom du ikke har satt regler som omgår dette. Du kan surfe på internett uten at noen ser deg, og du er også beskyttet mot DoS angrep.

- Kaspersky® Anti-Hacker teknologien oppfatter de mest brukte angrepsmåtene mot din datamaskin og blokkerer disse automatisk.
- Sikkerhetsnivåer er forhåndsdefinert av eksperter som enkelt lar deg velge den grad av sikkerhet du ønsker. Du kan velge mellom 5 nivåer fra fullstendig blokkering av all kommunikasjon, til mer spesifiserte innstillinger som sperrer kjente angrepsmåter. Kaspersky® Anti-Hacker tillater også at du lager dine egne regler for hvordan programmet skal håndtere kommunikasjon fra enkelte applikasjoner.

### **Kaspersky Security for PDA**

I dag bruker tusenvis av folk sine håndholdte og portable enheter til å lagre viktig informasjon, alt fra kredittkortnummer til intern bedriftsinformasjon verdt millioner av kroner. Uheldigvis, var den originale Palm-enheten designet som en personlig PDA (Personal Digital Assistant); derfor er den innebygde sikkerheten i PDA ikke god nok til å gi den sikkerheten som trengs. For å komme dette problemet til livs, har Kaspersky Labs spesielt laget Kaspersky® Security for PDA - et full-skala forsvar som gir pålitelig kontroll over tredjeparts tilgang til en beskyttet enhet, og hindrer informasjonslekkasje.

- Anti-virus beskyttelse for Windows CE skanner både datalager og minnekort. 'Datasafe' modulen muliggjør opprettelse av passordbeskyttede filer. Data i disse filene krypteres, og sikrer dermed at filene ikke kan benyttes av autoriserte brukere.
- Programmet overvåker alle datapakker som kan opptre som infiserte vektorer: skanning av datalager, RAM og minnekort beskytter deg mot infeksjoner gjennom HotSync og Beam. ' Datasafe' modulen gir deg også beskyttelse med passord og kryptering - og låser dermed enheten etter brukerspesifikasjon.

### **Kaspersky Anti-Virus Business Optimal**

Programpakken inneholder total beskyttelse for små og mellomstore bedrifters nettverk.

Kaspersky Anti-Virus Business Optimal inneholder beskyttelse for;

- *Arbeidsstasjoner* som kjører Windows 98/ME, Windows NT/2000/XP Workstation, og Linux;
- *Fil- og applikasjonsservere* som kjører Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD og OpenBSD, eller Linux;

- *E-post systemer*, Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, og Qmail;
- *Internett-gateways*: CheckPoint Firewall –1; Microsoft ISA Server.

Kaspersky Anti-Virus Business Optimal inneholder Kaspersky Administration Kit, et unikt verktøy for automatisert utrulling og administrasjon.

Bedriften kan selv velge hvilken av disse produktene de ønsker å benytte.

### **Kaspersky Corporate Suite**

Denne programpakken er en utvidet konfigurert sikkerhetspakke som er spesifikt designet for å beskytte store nettverk fra trusler. Med sin fleksible konfigurasjonsmulighet sikres dataintegritet for til og med de mest komplekse nettverk. Pakken har også en veldig fleksibel og skalerbar lisensieringspolitikk, som gjør at løsningen kan skreddersys konsernets behov og krav.

Sentralisert administrasjon er kjernen i all programvare som benyttes i store miljøer. Kaspersky Administration Kit utfører disse oppgavene til punkt og prikke - og inneholder et komplett sett med administrative verktøy for sentralisert administrasjon, konfigurering og overvåking av konsernets anti-virus beskyttelse.

Kaspersky Corporate Suite tilbyr omfattende beskyttelse for;

- *Arbeidsstasjoner* som kjører Windows 98/ME, Windows NT/2000/XP Workstation, og Linux;
- *Fil- og applikasjonsservere* som kjører Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD og OpenBSD, eller Linux;
- *E-post systemer*, Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim og Qmail;
- *Internett-gateways*: CheckPoint Firewall –1; Microsoft ISA Server;
- *Håndholdte og portable enheter* (PDAs).

Kaspersky Corporate Suite kommer med Kaspersky Administration Kit, et unikt verktøy for automatisk utrulling og administrering.

Organisasjonen kan selv velge hvilke av komponentene de ønsker å benytte.

### **Kaspersky Anti-Spam**

Kaspersky® Anti-Spam er et meget kraftig og fornuftig multispråklig system, som er dedikert til å stoppe forstyrrende e-post trafikk, fra et sentralt punkt - for større bedrifter og ISP'er. Systemets effektivitet baseres på samtidig bruk av svartelister (black-list), meldingseksempler og avansert heuristisk språkanalyse (intelligent innholdsanalyse). Kaspersky® Anti-Spam kan benyttes som et filter

for alle e-post systemer, og utvidet integrasjonsmulighet finnes for øyeblikket for Sendmail, Qmail, Postfix, Exim og Communigate Pro. Systemet kan installeres eksternt eller direkte på bedriftens e-post server (avhengig av systemløsning)

Mengden av spam - eller uønsket e-post - øker daglig. En innboks full av spam er ikke bare en plage men er også meget tidkrevende. Dette er kostbart for bedriften. Kaspersky® Anti-Spam gir ISP'er og bedrifter av alle størrelser en sentralisert effektiv beskyttelse mot uønsket e-post. Løsningen oppdager spam i innkommende e-post gjennom SMTP protokollen og filtrerer dette ut før e-posten leveres til mottakeren.

Regelmessige oppdateringer til lingvistikkdatabasen sikrer identifisering av spam. Disse oppdateringene blir laget av et dedikert lingvistikk team som overvåker og analyserer spamtrafikk hele døgnet. Resultatet blir brukt til å lage spesielle spam signaturer; Kaspersky® Anti-Spam sammenligner innkommende e-post mot disse signaturene. Oppdateringen publiseres annenhver time. Oppgraderingen av Kaspersky® Anti-Spam inkluderer også nye versjoner av lingvistikk-kjernen.

### **Kaspersky Anti-Spam Personal**

Kaspersky® Anti-Spam Personal er konstruert for sømløs integrasjon med din innboks, og for å beskytte din datamaskin mot alle mulig varianter av spam.

Kaspersky Anti-Spam Personal detekterer spam som hentes via protokollene POP3 og IMAP (bare Microsoft Outlook).

Regelmessige oppdateringer til lingvistikkdatabasen sikrer identifisering av spam. Disse oppdateringene blir laget av et dedikert lingvistikk team som overvåker og analyserer spamtrafikk hele døgnet. Resultatet blir brukt til å lage spesielle spam signaturer; Kaspersky® Anti-Spam sammenligner innkommende e-post mot disse signaturene. Oppdateringen publiseres annenhver time.

## **C.2. Kontaktinformasjon**

Dersom du har noen spørsmål, kommentarer eller forslag, ta gjerne kontakt med en av våre leverandører eller direkte til Kaspersky Lab. Vi hjelper deg gjerne med noen spørsmål du måtte ha om noen av våre produkter. Ta gjerne kontakt med oss på e-post eller telefon. Alle dine kommentarer og forslag vil bli gått nøye igjennom og vurdert.

## Norge

Brukerstøtte	Informasjon om brukerstøtte er tilgjengelig via våre nettsider: <a href="http://www.kaspersky.no/support">http://www.kaspersky.no/support</a>
Generell informasjon	WWW: <a href="http://www.kaspersky.no">http://www.kaspersky.no</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-postl: <a href="mailto:info@kaspersky.no">info@kaspersky.no</a>

## Internasjonalt

Brukerstøtte	Informasjon om brukerstøtte er tilgjengelig via våre nettsider: <a href="http://www.kaspersky.com/support">http://www.kaspersky.com/support</a>
Generell informasjon	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-post: <a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>

---

# APPENDIX D. LISENSAVTALE

## Standard lisensavtale for sluttbrukere

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB. ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD SLEEVE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE. YOU MAY RETURN THIS SOFTWARE FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN AUTHORISED KASPERSKY LAB DISTRIBUTOR OR RESELLER. THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. Licence Grant. Subject to the payment of the applicable licence fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software produce, this licence applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This licence authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You will maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorised copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to human readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab on request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability provided that you may only reverse engineer or decompile to the extent permitted by law.

1.1.4 You shall not, make error corrections to or otherwise modify, adapt or translate the Software nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein)

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-licence your licence rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on or as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate licence is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licenced Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licences required (i.e., the required number of licences would equal the number

of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licences you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licence you have obtained. This licence authorises you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licences. If the Software is licensed with volume licence terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume licence terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licences you have obtained. This licence authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume licence, provided that each such copy contains all of the Document's proprietary notices.

2. Term. This Agreement is effective for one (1) year unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

### 3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year on:

(a) Payment of its then current support charge; and

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy which is attached to this Agreement, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means

(a) Daily updates of anti-virus databases;

(b) Free software updates, including version upgrades;

(c) Extended technical support via email and hot phone-line provided by Vendor and/or Reseller;

(d) Virus detection and curing updates in 24-hours period.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

#### 6. Limited Warranty

(i) Kaspersky Lab warrants that for 90 days from first download or installation the Software will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted and error free;

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected with that virus;

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item;

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended or (c) use the Software other than as permitted under this Agreement;

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (v) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

## 7. Limitation of Liability

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (i) the tort of deceit, (ii) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), the Supplier shall have no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data; or

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraph (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the Kaspersky Lab's liability (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the

Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (i) This Agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii), you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made by it knowing that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as to a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).