

# SIKKERHET PÅ PC

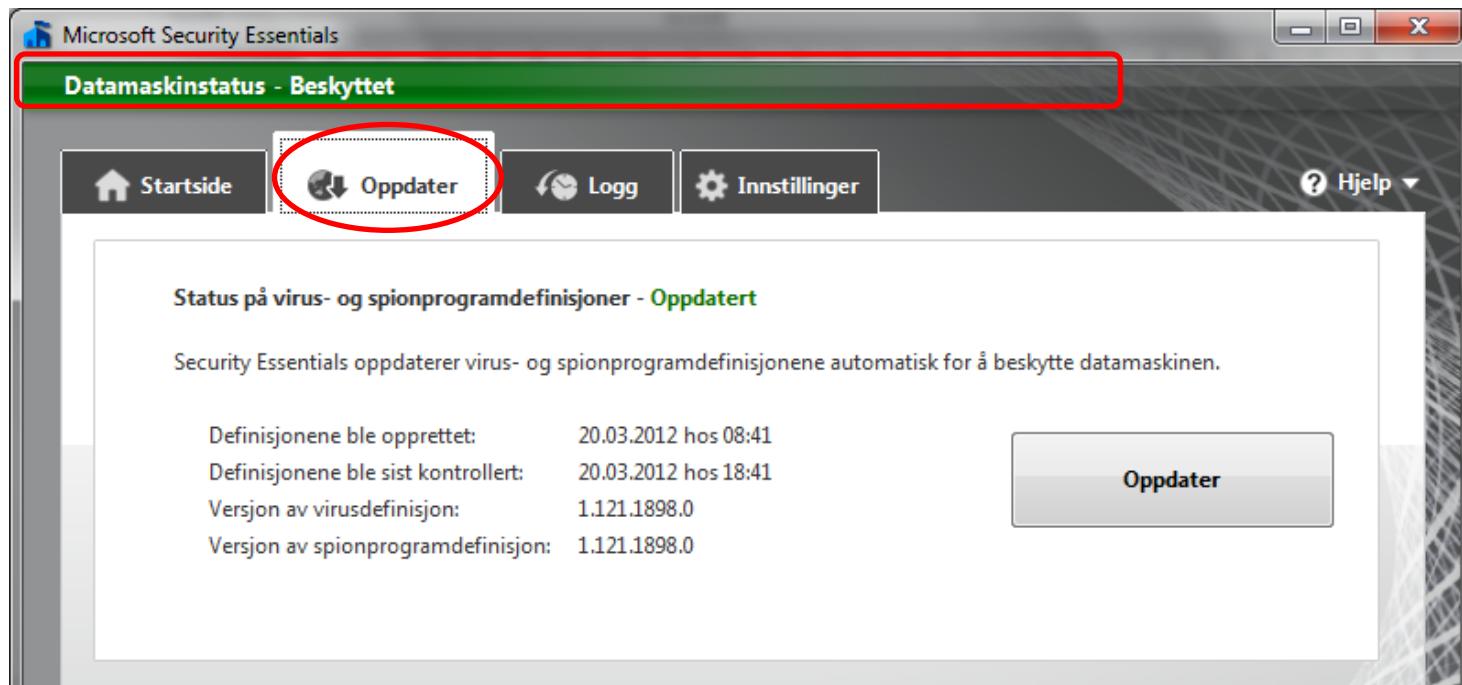
## 12 tips til sikrere PC

1. Installer antivirusprogram, oppdater den og aldri installer 2 antivirusprogrammer samtidig
2. Kjør Windows Update/Microsoft Update manuelt og sørg for at alt er installert. Slå på Automatisk oppdatering i Window (Windows Update – Endre innstillinger)
3. Start Handlingssenter/Sikkerhetscenter i Kontrollpanel og kontroller sikkerhetsstatusen i Windows. Følg instruksjonene ved advarsler
4. Bruk passord som er en blanding av små og store tegn og som inneholder både tall og bokstaver
5. BRUK SUNN FORNUFT!!! Ikke gå på mistenkelige meldinger fra bl.a. banker. Skriv navn til nettstedet direkte inn i adressefeltet.
6. Oppdater alle programmer du bruker på PC-en din (Acrobat Reader, Java, Media Player)
7. Se til at du bruker sikker nettside for nettbank og andre nettsider der du har mulighet for det
8. Installer tilleggsprogrammer for ekstra sikkerhet (Antimalware, Antispyware)
9. Ikke lar deg lure av nettsteder og spam e-poster som lurer deg til å installere ukjent programvare for å fjerne virus eller spionprogrammer.
10. Kontroller alltid innstillinger for programmer du bruker
11. Installer program for overvåking av «helsetilstanden» til programmer på din PC
12. Sikker avinstallering av programmer på PC

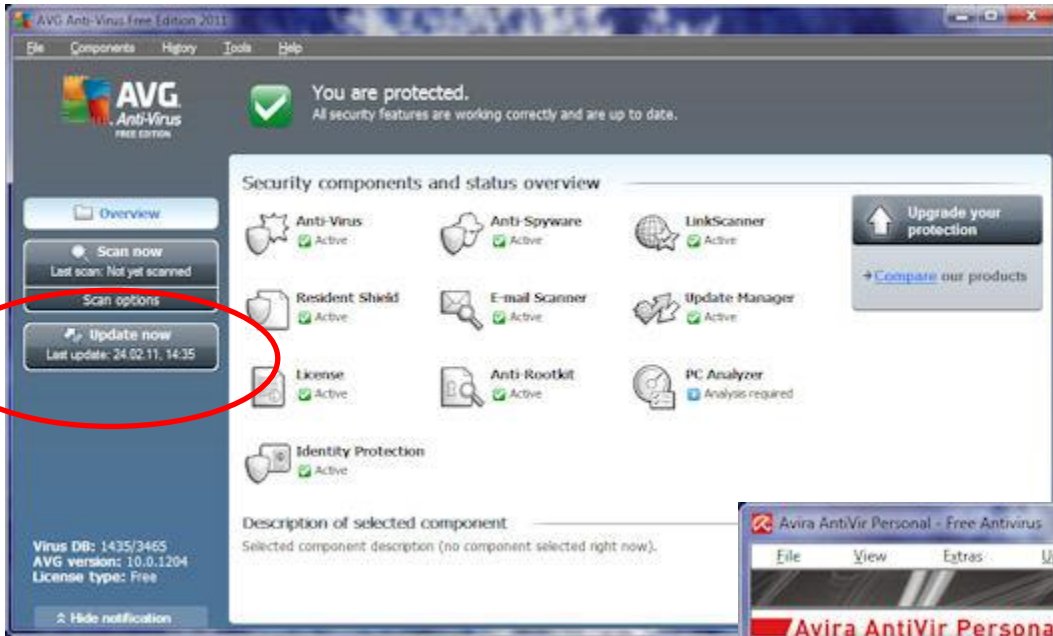
# 1 .Installer antivirusprogram og oppdater den

- Oppdateringer gjelder for alle programmer på din PC, men det er spesielt viktig for f.eks. ditt antivirus program
- Mange antivirusprogrammer som f.eks. Microsoft Security Essentials har automatisk oppdatering. Sjekk hvordan det er for antivirusprogram du har på din PC. Åpne ditt antivirusprogram og fin valget for oppdatering.

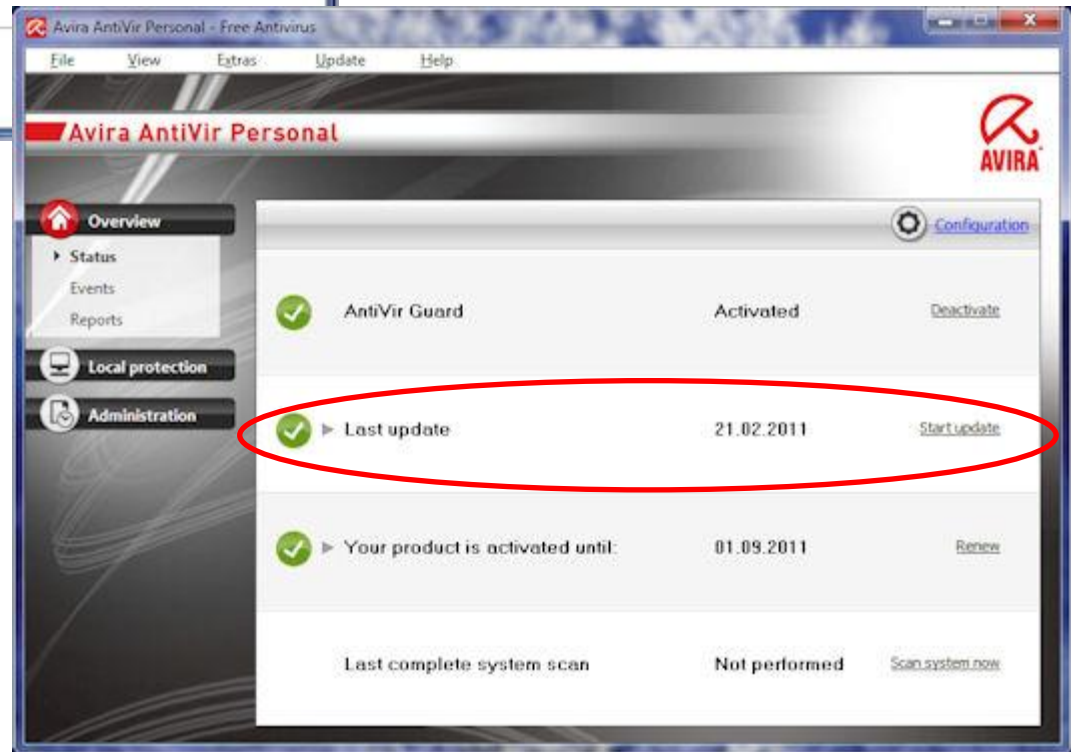
## Microsoft Security Essentials



# AVG



# AVIRA



## Kort om virus, trojanere og ormer

- **Et virus:** er en del av en datakode som knytter seg selv til et program eller en fil, slik at det kan spre seg fra datamaskin til datamaskin. Det infiserer mens det overføres. Virus kan ødelegge programvaren, maskinvaren og filene.

Den gode nyheten er at et ekte virus ikke sprer seg uten brukermedvirkning. Noen må dele en fil eller sende en e-post for å føre det videre.

- **Orm:** en undergruppe av virus. En orm sprer seg generelt uten brukermedvirkning og distribuerer fullstendige kopier (muligens endrede) av seg selv på tvers av nettverk. En orm kan bruke mye minne eller nettverksbåndbredde, noe som kan føre til at datamaskinen krasjer. Fordi ormer ikke må overføres via et "vertsprogram" eller en fil, kan de også trenge inn i systemet og la andre ta ekstern kontroll over datamaskinen.
- **Trojansk hest:** et dataprogram som gir inntrykk av å være nyttig, men som faktisk gjør skade. Trojanske hester sprer seg når folk lokkes til å åpne et program fordi de tror det kommer fra en legitim kilde. Trojanske hester kan også inkluderes i programvare som kan lastes ned gratis. Last aldri ned programvare fra en kilde som du ikke stoler på.

- **AVG**

- + Gratis

- + Lite ressurskrevende

- Tungvint og langvarig installasjon

- For mange sprettoppvinduer

- Programmet fant trolig falsk positiv

- Har flere funksjoner enn vi setter pris på

- Tungvint opplegg for fjerning av virus

- Dårlig effektivitet - finner få trusler

- **Microsoft Security Essentials**

- + Brukervennlig

- + Tilbyr sanntidsbeskyttelse

- + Effektivt mot skadelige programmer

- Virusskanning tar lang tid

- **Avast**

- + Gratis

- + Ikke ressurskrevende

- + Programmet har Stille/spill-modus for å slå av varsler

- + Innebygd sanntidsbeskyttelse og selvforsvar

- + Finnes i norsk språkversjon

- Ikke spesielt brukervennlig

- Mye mas med sprettoppvinduer

- Dårlig effektivitet

- Gir ikke detaljer om trusler som blir funnet

- **Avira**

- + Gratis

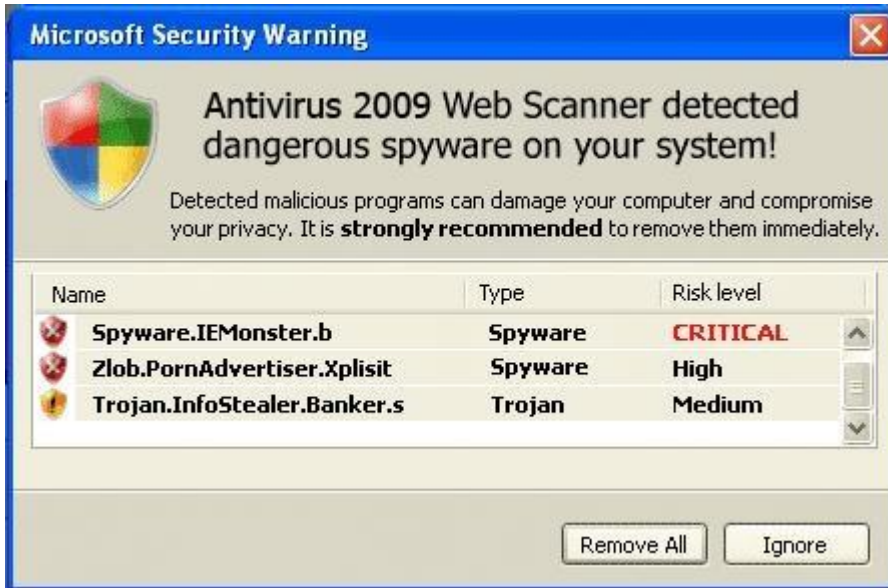
- + Ikke ressurskrevende når det kjører i bakgrunnen

- + God effektivitet ved å finne og fjerne virus

- Brukergrensesnittet kunne vært enklere

- Programmet må aktiveres på nytt om seks måneder

## Falske antivirusprogrammer og sikkerhetssentere lurere deg



Maskinen din kan lett bli infisert av en trojaner. Det kan være så enkelt at du klikker på en lenke på en facebook-profil, at du mottar en e-post med infiserte vedlegg - eller at du rett og slett er innom sider som laster inn trojaneren uten at du oppdager det. Etter at maskinen er blitt infisert, begynner det falske antivirusprogrammet å gi deg falsk informasjon

Vi stoler på at antivirusprogrammet, brannmuren og operativsystemet som er installert på maskinen gir oss beskjed dersom det er noe galt eller vi er blitt infisert.


Det gjør at vi blir mindre årvåkne og stoler på de beskjedene vi får fra antivirusprogrammet og sikkerhetssenteret på datamaskinen - uten tanke på at beskjedene vi får kan være falske.

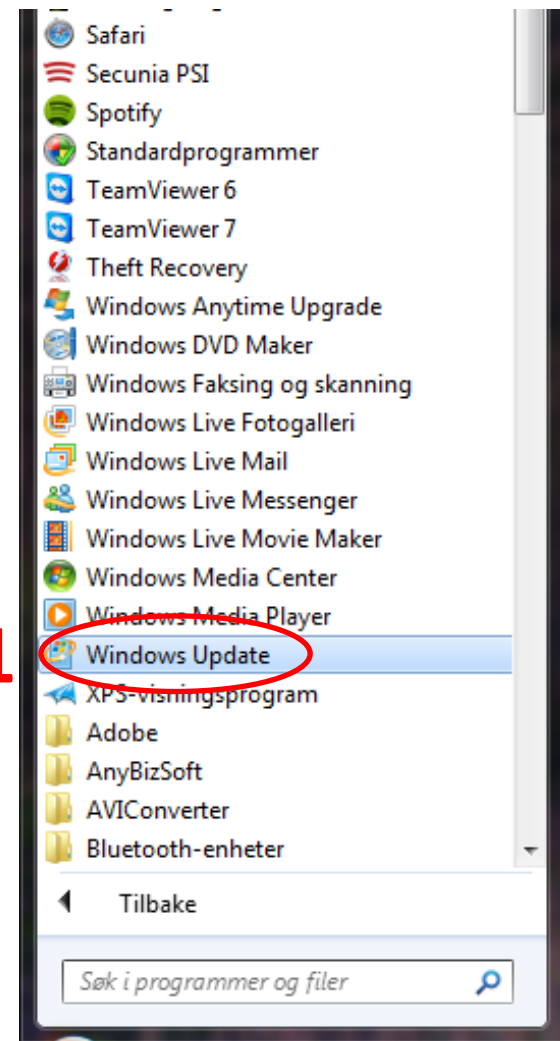
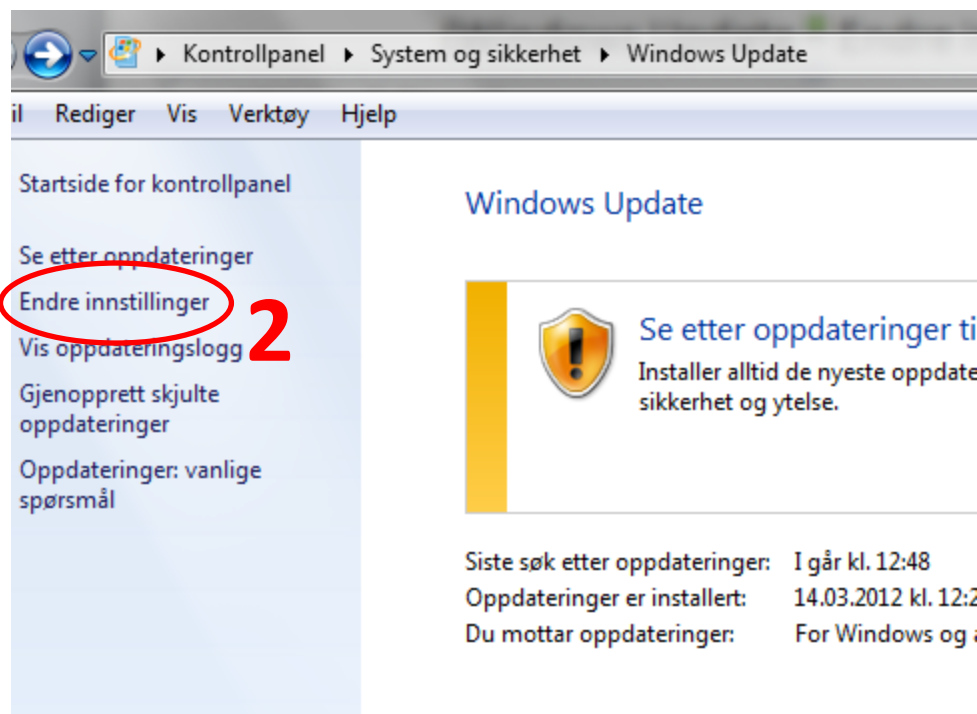
Hvis du er uoppmerksom og kjøper en falsk oppdatering eller aktivering av sikkerhetsprogramvare, koster det som oftest mellom fem og ti dollar.

Det skjer som regel ingenting merkbart med datamaskinen din i etterkant. Problemet ditt er at du har gitt kredittkortnummeret ditt til svindlerne, slik at de kan bruke informasjonen til å tappe kontoen din for penger.

En sikkerhetsrapport fra Microsoft viser at falske antivirusprogram, eller "fake security center" som de også kalles, er blant et av de tre mest vanlige virusangrepene på datamaskiner.

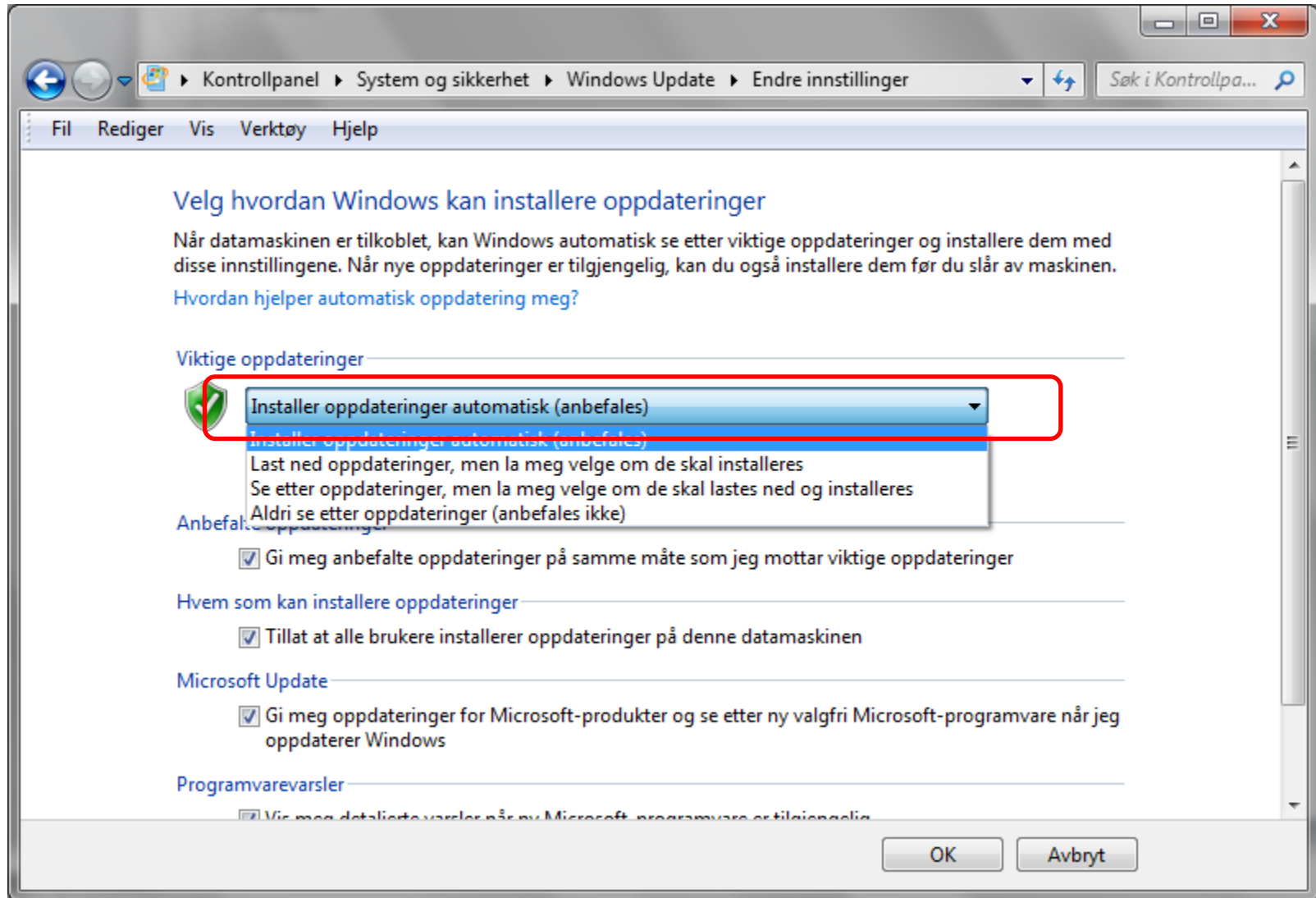
## 2. Kjør Windows Update/Microsoft Update manuelt og sørg for at alt er installert. Slå på Automatisk oppdatering (Windows Update – Endre innstillinger)

- Klikk på  Startknappen
- Velg «Alle programmer»
- Finn «Windows update» og klikk på den (1)
- Velg «Endre Innstillinger» (2)




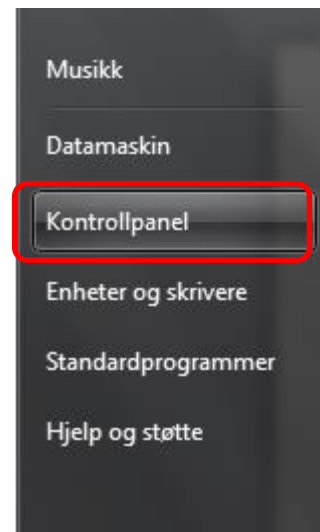
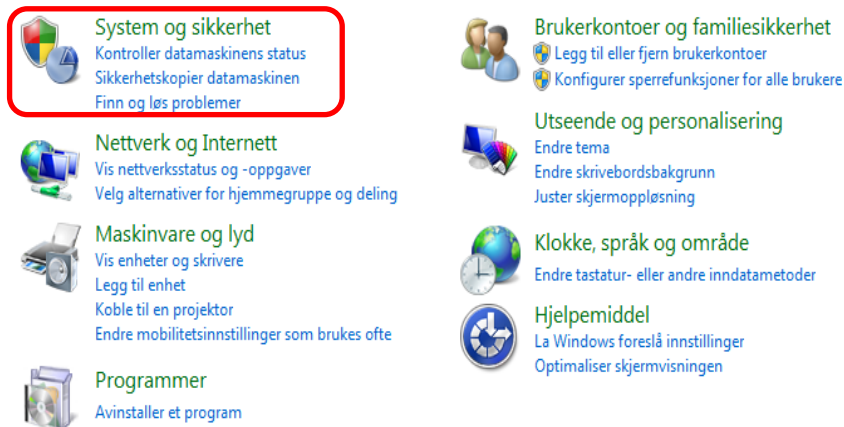


- Velg fra rullegardinen «Installer oppdateringer automatisk» og trykk OK

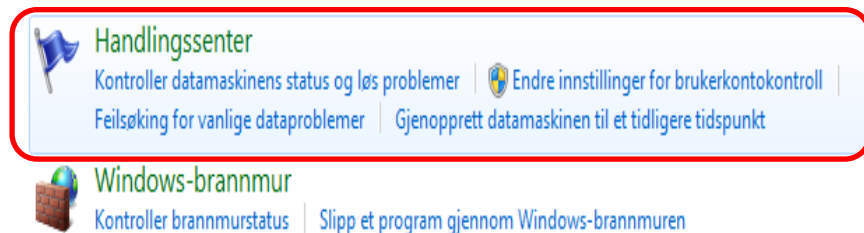



### 3. Start Handlingscenter/Sikkerhetscenter i Kontrollpanel og kontroller sikkerhetsstatusen i Windows. Følg instruksjonene ved advarsler

- Dersom du har **Windows 7**
- Klikk på «Startknappen»  og velg «Kontrollpanel»
- Kontrollpanel åpner med 8 kategorier og du velger kategori «System og Sikkerhet»



og deretter «Handlingscenter»



- Klikk på piltast til høyre for «Sikkerhet» (1), så kommer sikkerhetsvalgene frem. Kontroller om det er som nedenfor.
- \* «Brukerkontroll» (2) kan også stå på «Av» (klikk da på  Endre innstillinger )
- Ønsker du å endre innstillinger – klikk «Endre innstillinger for Handlingscenter» (3)

Startside for kontrollpanel

Se gjennom nylig innlagte meldinger og løs problemer

Handlingscenter oppdaget ingen problemer.

**(3)** [Endre innstillinger for Handlingscenter](#)

[Endre innstillinger for brukerkontroll](#)

[Vis arkiverte meldinger](#)

[Vis ytelsesinformasjon](#)

**(1)** 

### Sikkerhet

Nettverksbrannmur	På
 Windows-brannmuren beskytter datamaskinen aktivt.	
Windows Update	På
Windows installerer oppdateringer automatisk når de blir tilgjengelige.	
Virusbeskyttelse	På
Det rapporteres at Microsoft Security Essentials er oppdatert, og at virusøk er aktivert.	
Beskyttelse mot spionprogrammer og uønsket programvare	På
Det rapporteres at Microsoft Security Essentials er aktivert.	
<a href="#">Vis installerte antispionvareprogrammer</a>	
Sikkerhetsinnstillinger for Internett	OK
Alle sikkerhetsinnstillinger for Internett er satt til anbefalt nivå.	
<b>(2)</b> Brukerkontroll	På
DAC varsler alltid, og venter på svar.	
 <a href="#">Endre innstillinger</a>	
Beskyttelse av nettverkstilgang (NAP)	Av
Agenttjenesten for Beskyttelse av nettverkstilgang kjører ikke	
<a href="#">Hva er Beskyttelse av nettverkstilgang?</a>	

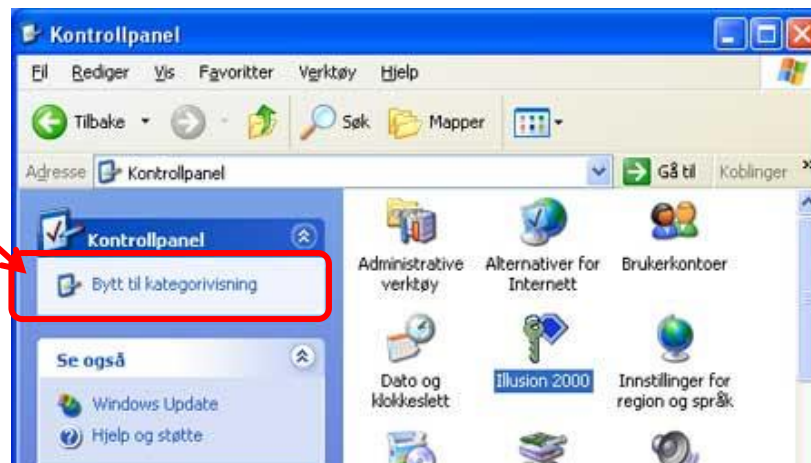
Dersom du har **Windows XP**

- Klikk på «Startknappen»  
og velg «Kontrollpanel»



- Kontrollpanel vises i «Kategorivisning».

Dersom det viser i ikoner som vist nedenfor – klikk på «Bytt til kategorivisning»




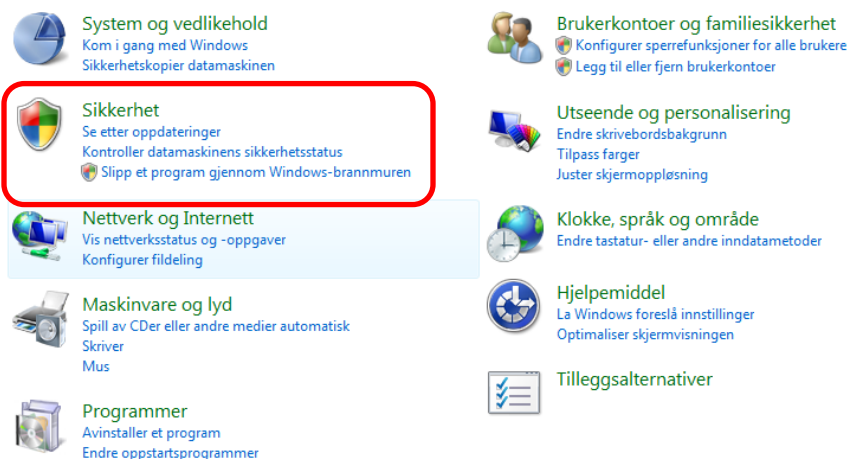
- Velg «Sikkerhetscenter»



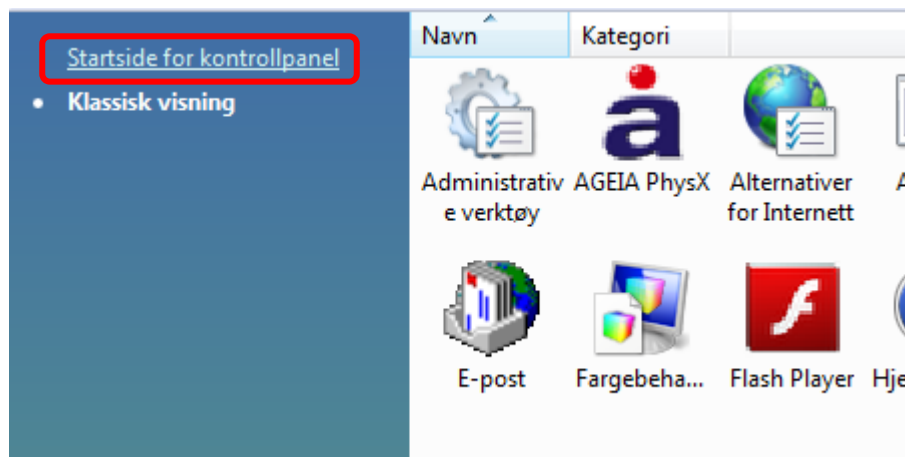
- I sikkerhetscenter kan du administrere sikkerhetsinnstillinger for «Windows Brannmur», «Alternativer for Internett –sikkerhet» og «Automatiske oppdateringer»

# Dersom du har Windows Vista

- Klikk på «Startknappen»  og velg «Kontrollpanel»
- Kontrollpanel åpner seg i Kategorivisning (som nedenfor). Velg «Sikkerhet»




\* Dersom kontrollpanel åpnes med Ikon-visning (som nedenfor), klikk på «Startside for kontrollpanel» Så kommer du til Kategorivisning og velger «Sikkerhet»



- Velg «Sikkerhetssenter»



### Sikkerhetssenter

Se etter oppdateringer | Kontroller datamaskinens sikkerhetsstatus |  
Slå automatisk oppdatering på eller av |  Kontroller brannmurstatus  
Krev passord når datamaskinen reaktiveres



### Windows-brannmur

 Slå Windows-brannmuren på eller av |  Slipp et program gjennom Windows-brannmuren



### Windows Update

Slå automatisk oppdatering på eller av | Se etter oppdateringer | Vis installerte oppdateringer



### Windows Defender

Søk etter spionprogrammer og annen mulig uønsket programvare



### Alternativer for Internett

Endre sikkerhetsinnstillinger | Slett webleserlogg og informasjonskapsler | Behandle weblesertillegg



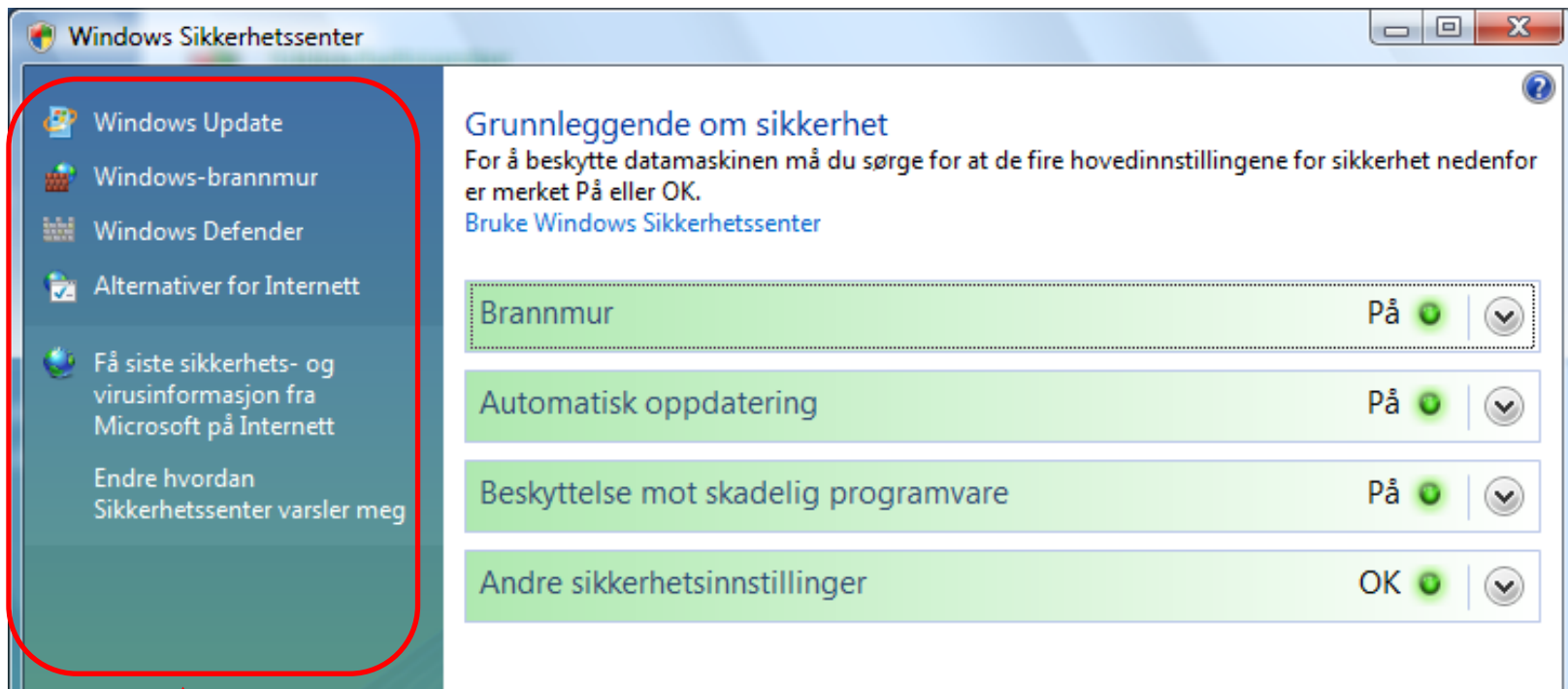
### Sperrefunksjoner

 Konfigurer sperrefunksjoner for alle brukere |  Vis aktivitetsrapporter



### Flash Player

- I «Windows sikkerhetssenter» kan du kontrollere om de viktige sikkerhetsfunksjoner som bl.a. Brannmur, Beskyttelse mot skadelige programvare er slått på.



- På venstre side er det også valg for andre sikkerhetsfunksjoner som Windows Update og Alternativer for Internett



## 4. Bruk passord som er en blanding av små og store tegn og som inneholder både tall og bokstaver

- Passord skal være lett å huske for deg men samtidig vanskelig å gjette for andre
- Ideelt skal passordet ha en blanding av bokstaver (helst blanding av store og små) og tall
- Lag ett god og sikkert passord til f.eks. nettbank, MinID, Altinn osv. ; det betyr at f.eks. fornavn, etternavn eller navn til ditt kjæledyr ikke er trygg og sikkert  
For de programmer/sider der det ikke settes så store krav til sikkerhet kan en velge et mer enkelt passord
- Det å huske mange forskjellige passord er et stort problem.  
Dersom du gir alle programmer et forskjellig passord, kan det lett bli mye krøll
- Det viktige er at passordet skal være logisk for deg men ikke for andre .

## 5. BRUK SUNN FORNUFT!!! Ikke gå på mistenkelige e-poster eller meldinger fra bl.a. banker. Skriv navn til nettstedet direkte inn i adressefeltet.

- Nedenfor vises 2 eksempler av e-poster som er mistenkelige, og som prøver å lure deg.

### Banker sender deg ALDRI slike typer e-post

Kære kunde Nordea

Du har 1 New Security besked!

Du har mottatt denne filen fordi din SpareBank Konto har blitt midlertidig suspendert.

[Klik her for at løse problemet](#)

Takk for at du bruker SpareBank 1

| SpareBank 1 Gruppen AS. | Personvern og vilkar for bruk av nettsidene. |

Kjære kunde SpareBank 1

Du har 1 New Security beskjed!

Du har mottatt denne filen fordi din SpareBank Konto har blitt midlertidig suspendert.

[Klikk her for å løse problemet](#)

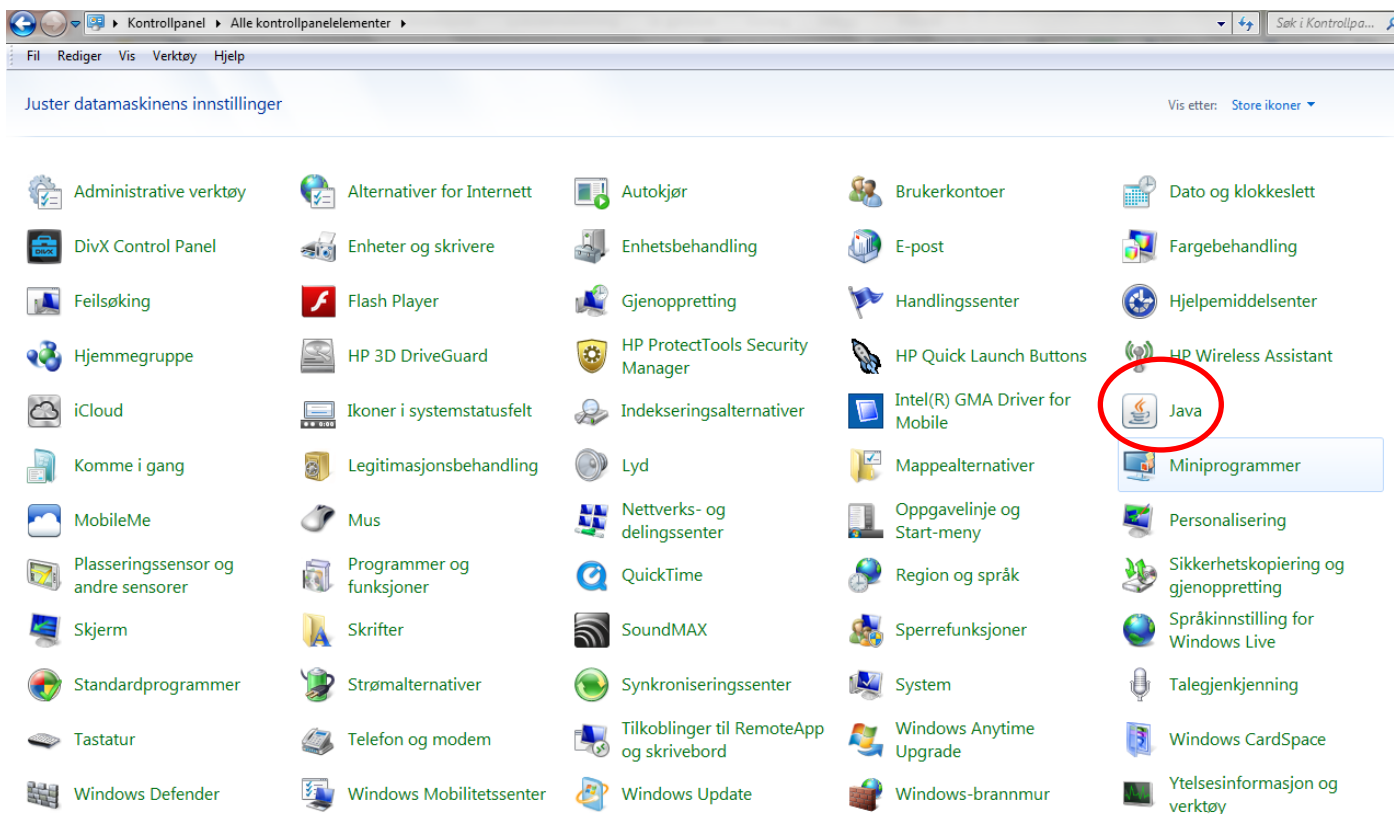
Takk for at du bruker SpareBank 1

| SpareBank 1 Gruppen AS. | Personvern og vilkår for bruk av nettsidene. |

## 6. Oppdater alle programmer du bruker på PC-en din ( f.eks. Java, Acrobat Reader og Media Player)









- Nedenfor vises noen eksempler på hvordan du oppdaterer programmer som ikke kan settes til automatisk oppdatering (som Java, Acrobat Reader og Media Player)

**Java:** Klikk på «Startknappen» og velg «Kontrollpanell» Vises kontrollpanel i «Ikoner», vil du finne «Java». Klikk på «Java»



- Viser den i «Kategori visning» : klikk på «Programmer»

Juster datamaskinens innstillinger Vis etter: Kategori ▾

 <p><b>System og sikkerhet</b> Kontroller datamaskinens status Sikkerhetskopier datamaskinen Finn og løs problemer</p>	 <p><b>Brukerkontoer og familiesikkerhet</b> Legg til eller fjern brukerkontoer Konfigurer sperrefunksjoner for alle brukere</p>
 <p><b>Nettverk og Internett</b> Vis nettverksstatus og -oppgaver Velg alternativer for hjemmegruppe og deling</p>	 <p><b>Utseende og personalisering</b> Endre tema Endre skrivebordsbakgrunn Juster skjermoppløsning</p>
 <p><b>Maskinvare og lyd</b> Vis enheter og skrivere Legg til enhet Koble til en projektor Endre mobilitetsinnstillinger som brukes ofte</p>	 <p><b>Klokke, språk og område</b> Endre tastatur- eller andre inndatametoder</p>
 <p><b>Programmer</b> Avinstaller et program</p>	 <p><b>Hjelpemiddel</b> La Windows foreslå innstillinger Optimaliser skjermvisningen</p>

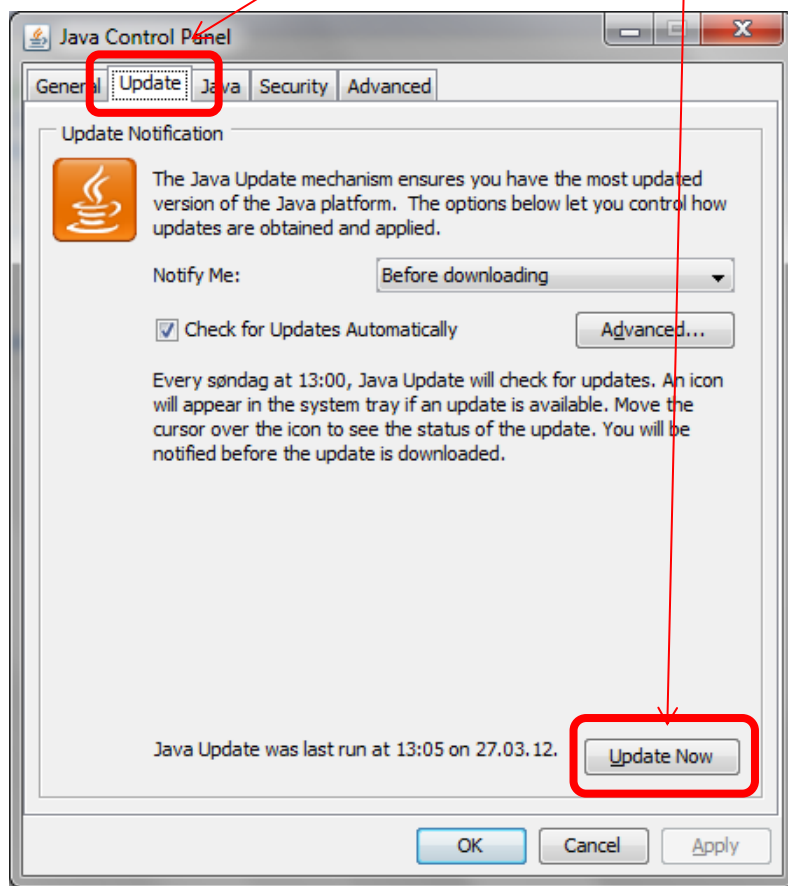
- Da finner du «Java» her. Klikk på «Java»

Startside for kontrollpanel

- System og sikkerhet
- Nettverk og Internett
- Maskinvare og lyd
- **Programmer**
- Brukerkontoer og familiesikkerhet
- Utseende og personalisering
- Klokke, språk og område
- Hjelpemiddel

 <p><b>Programmer og funksjoner</b> Avinstaller et program   Slå Windows-funksjoner på eller av   Vis installerte oppdateringer   Kjør programmer laget for tidligere Windows-versjoner   Hvordan installere et program</p>
 <p><b>Standardprogrammer</b> Endre standardinnstillinger for medier eller enheter   Få en filtype til å alltid åpnes i et bestemt program   Angi standardprogrammer</p>
 <p><b>Miniprogrammer</b> Legg til miniprogrammer på skrivebordet   Hent flere miniprogrammer på Internett   Avinstaller et miniprogram   Gjenopprett miniprogrammer som er installert med Windows</p>
 <p><b>Java</b></p>

- Følgende vindu kommer fram.  
Velg fanen «Update» og velg «Update Now»



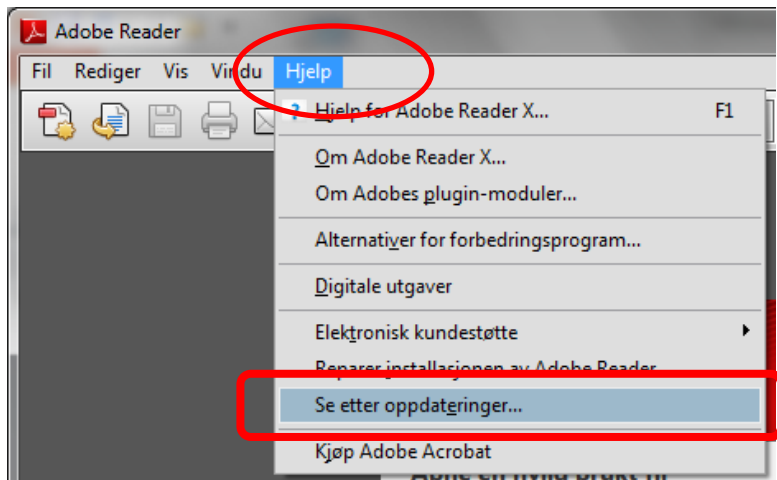
Installer eventuelle oppdateringer!

Dersom du har den siste versjon av Java, vil du få beskjed om dette.

## Acrobat Reader:

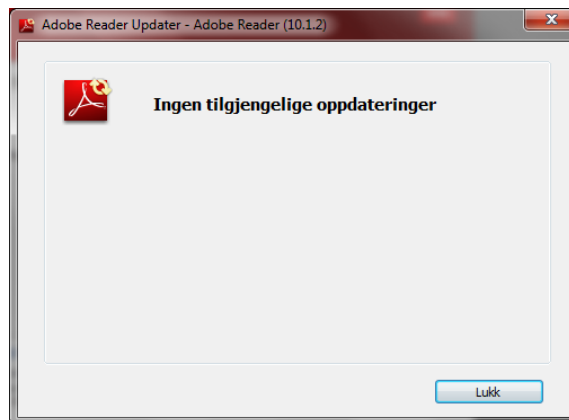
Klikk på «Startknappen» og velg «Alle Programmer» og velg «Acrobat Reader»

Klikk på «Hjelp» og velg «Se etter oppdateringer»



Dersom det er oppdateringen tilgjengelig, bør disse velges (OK).

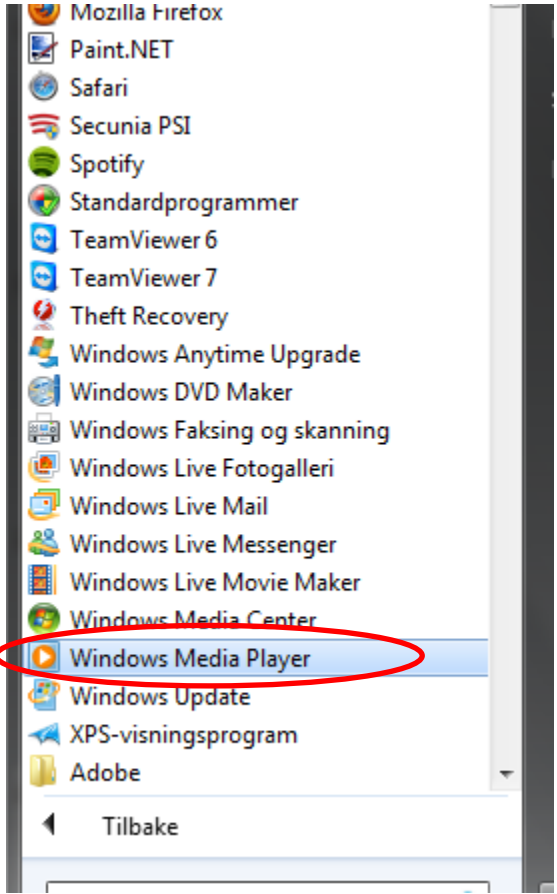
Dersom det er ingen oppdateringer får du følgende melding:



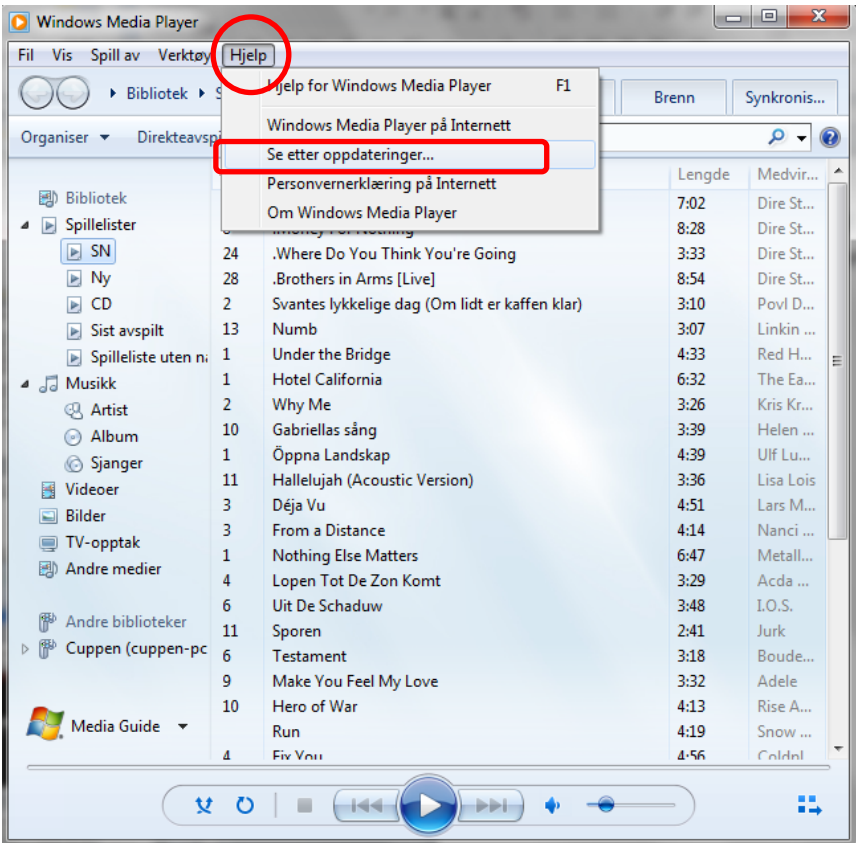
- **Media Player:**

Klikk på «Startknappen» og velg «Alle Programmer»

Finn «Windows Media Player» og klikk på den.

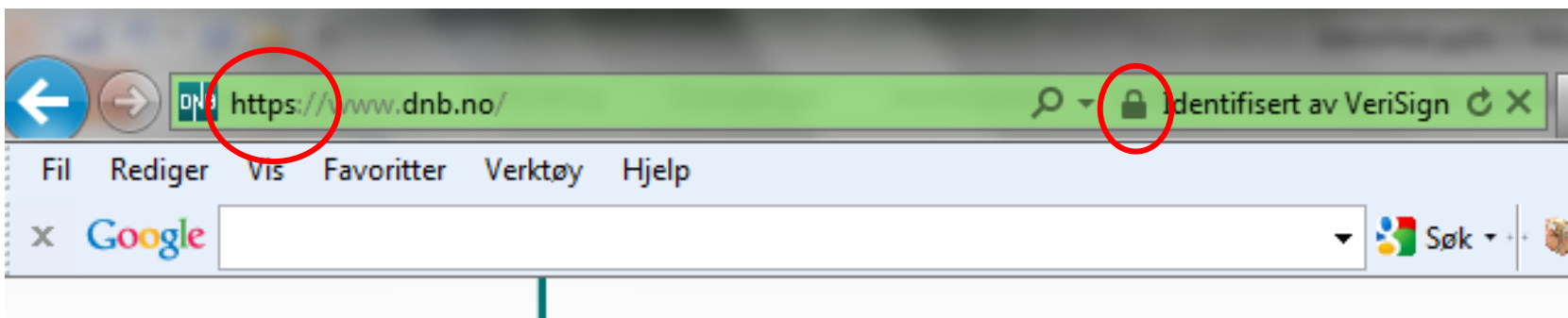


Klikk på «Hjelp» og velg «Se etter oppdateringer»  
Installer eventuelle oppdateringer.

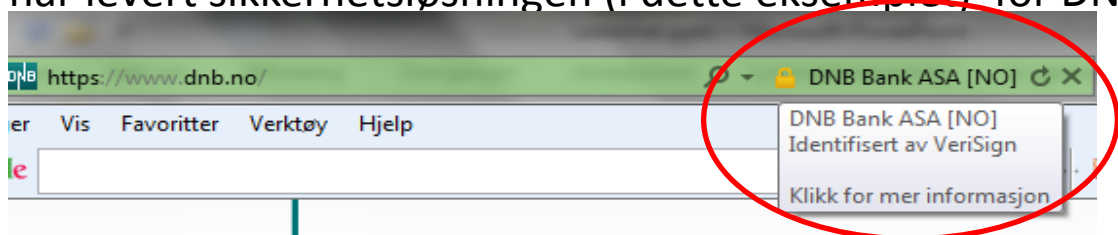


## 7. Se til at du bruker sikker nettside for nettbank (og andre sikre nettsider som f.eks. Facebook)

- Eksempelet her er nettbank fra DNB. Løsningen er den samme for alle norske nettbanker.
- Sikker nettside ser du i adressefeltet. Den har et par kjennetegn
- Først og fremst er det **https** som første 5 bokstaver i adressefeltet
- Så er det «hengelåsen» i adressefeltet.



- Setter du musepekeren på hengelåsen vil den «lyse opp» og vil det komme frem et lite vindu som sier hvem som har levert sikkerhetsløsningen (i dette eksemplet) for DNB Bank



- I tillegg har adressefeltet blitt farget, i dette eksemplet er adressefeltet grønt.
- Obs! Facebook har ikke farget adressefelt.



## 8. Installer tilleggsprogrammer for ekstra sikkerhet som f.eks. Antimalware og Antispyware

- Antimalware program kan du laste ned gratis fra Malwarebyte  
<http://www.malwarebytes.org/>

Du kommer til nettsiden for nedlasting av Malwarebytes.

Klikk på «Download Now» («Buy Now» er mer løsningen for bedrifter)

På neste siden klikk igjen på «Download Now»

Klikk «Kjør» og følg anvisninger på skjermen

- Antispyware program kan du laste ned gratis fra Superantispyware  
[www.superantispyware.com/](http://www.superantispyware.com/)

Du kommer til nettsiden for nedlasting av Superantispyware

Klikk på «Free Edition Download»

Klikk deretter på «Kjør» og følg anvisninger på skjermen

9. Ikke lar deg lure av nettstedet og spam e-poster som lurer deg til å installere ukjent programvare for å fjerne virus eller spionprogrammer.

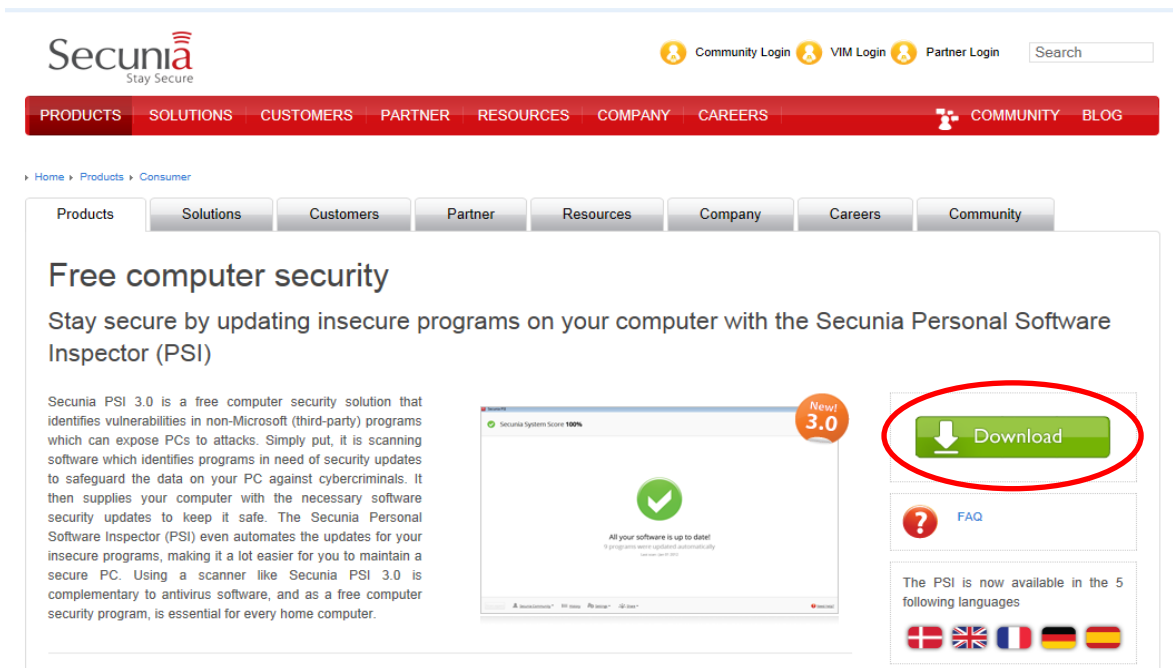
- Åpne bare e-post fra de du kjenner
- Åpne bare vedlegg du stoler på eller vedlegg som virker logisk og har et logisk navn
- E-posten virker mistenkelig selv om den er sendt av en du kjenner. Det er mistenkelig når emne eller vedlegget:
  - har et langt navn med mange bokstaver og tall blandet
  - har et navn som «Check this», «Are you interested», «Business registration» eller lignende
- Dersom du er i tvil, ta kontakt med den som sendte deg e-posten (selv om det er en du kjenner).

## 10. Kontroller innstillinger i programmer

- Kontroller alltid innstillinger i (nye) programmer
- Det er bl.a. kontoinnstillinger, personverninnstillinger og innstilling for sikker nettsurfing
- Innstillinger lar programmet kjøre som du ønsker

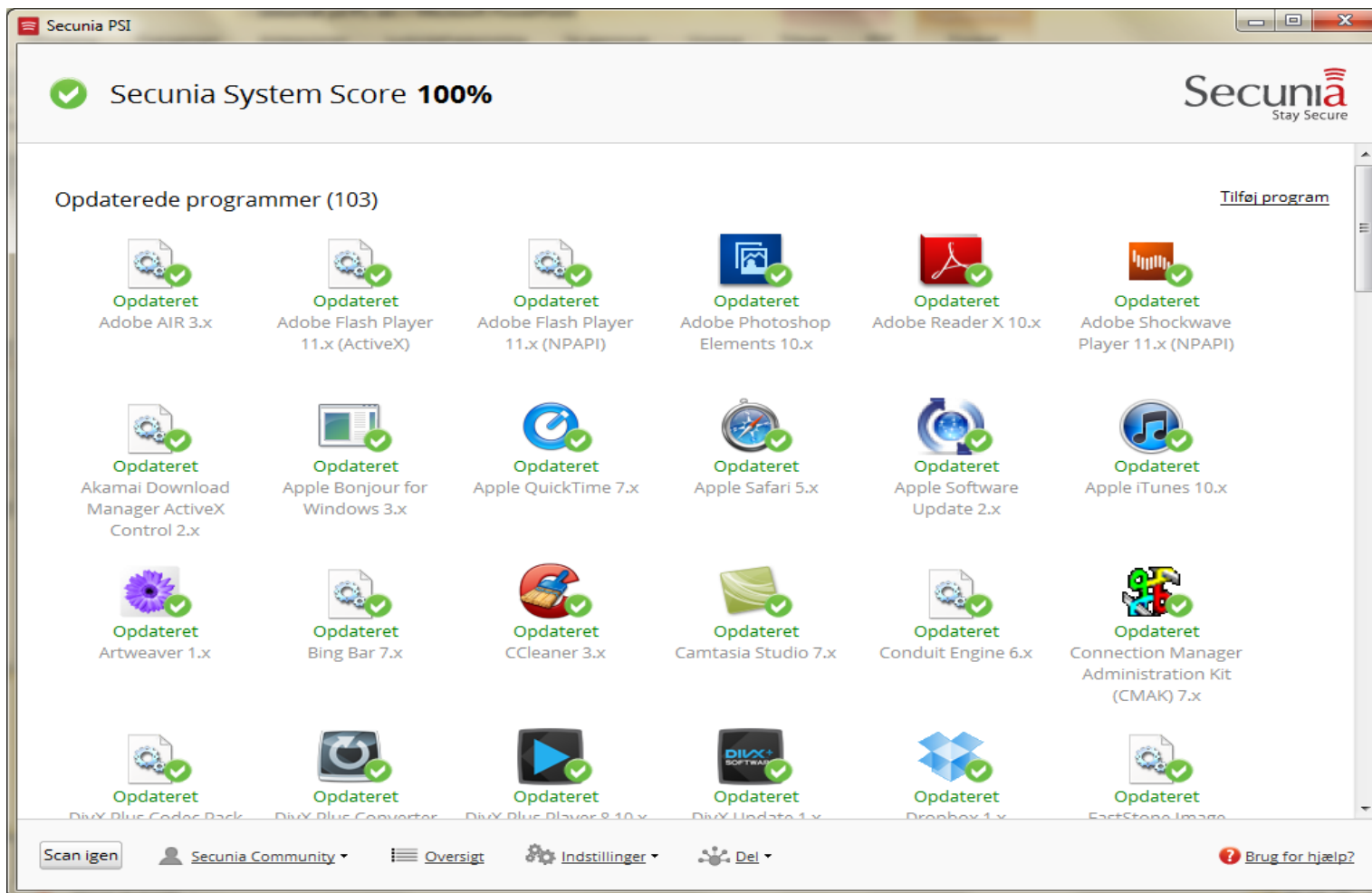
# 11. Installer program for overvåking av «helsetilstanden» til programmer på din PC – Secunia PSI

- Secunia PSI (Personal Software Inspector) er et program som skanner PC-en din bl.a. for å finne ut om alle programmer du har på din PC er oppdaterte
- Last ned Secunia PSI fra <http://secunia.com/products/consumer/psi/> og følg anvisninger i selve installasjonsprosessen



The screenshot shows the Secunia website's 'Free computer security' page. The page features a navigation bar with 'PRODUCTS', 'SOLUTIONS', 'CUSTOMERS', 'PARTNER', 'RESOURCES', 'COMPANY', 'CAREERS', 'COMMUNITY', and 'BLOG'. Below the navigation, there are tabs for 'Products', 'Solutions', 'Customers', 'Partner', 'Resources', 'Company', 'Careers', and 'Community'. The main content area is titled 'Free computer security' and includes the text: 'Stay secure by updating insecure programs on your computer with the Secunia Personal Software Inspector (PSI)'. A paragraph describes Secunia PSI 3.0 as a free computer security solution that identifies vulnerabilities in non-Microsoft programs. To the right of the text is a screenshot of the Secunia PSI interface showing a 'Security System Score 100%' and a green checkmark. A 'New! 3.0' badge is visible in the top right corner of the screenshot. Below the screenshot is a green 'Download' button with a white download icon, which is circled in red. Further down, there is a 'FAQ' link and a section titled 'The PSI is now available in the 5 following languages' with flags for Denmark, United Kingdom, France, Germany, and Spain.

- Hver gang Secunia startes opp vil den foreta en scan av din PC
- Slik ser programmet ut når det starter. I dette tilfelle er alle programmer oppdatert (har god helse). Da viser Secunia System Score 100%
- Dersom det ikke er 100% vil Secunia PSI begynne å søke etter oppdateringer for de programmer som trenger det



## 12. Sikker avinstallering av programmer på PC

- For en sikker og fullstendig avinstallering av programmer fra din PC kan du bruke programmet REVO-uninstaller.
- Last ned Revo-uninstaller fra <http://www.revouninstaller.com/revouninstallerfree/download.html>

Revo Uninstaller Pro  
Remove unwanted programs and traces easily

EASY TO USE  
FULL NATIVE SUPPORT OF 64BIT  
FORCED UNINSTALL

DOWNLOAD

Revo Uninstaller Pro

Download Revo Uninstaller Freeware and Professional

Revo Uninstaller Professional is a FULLY FUNCTIONAL TRIAL - 30 DAYS FREE!

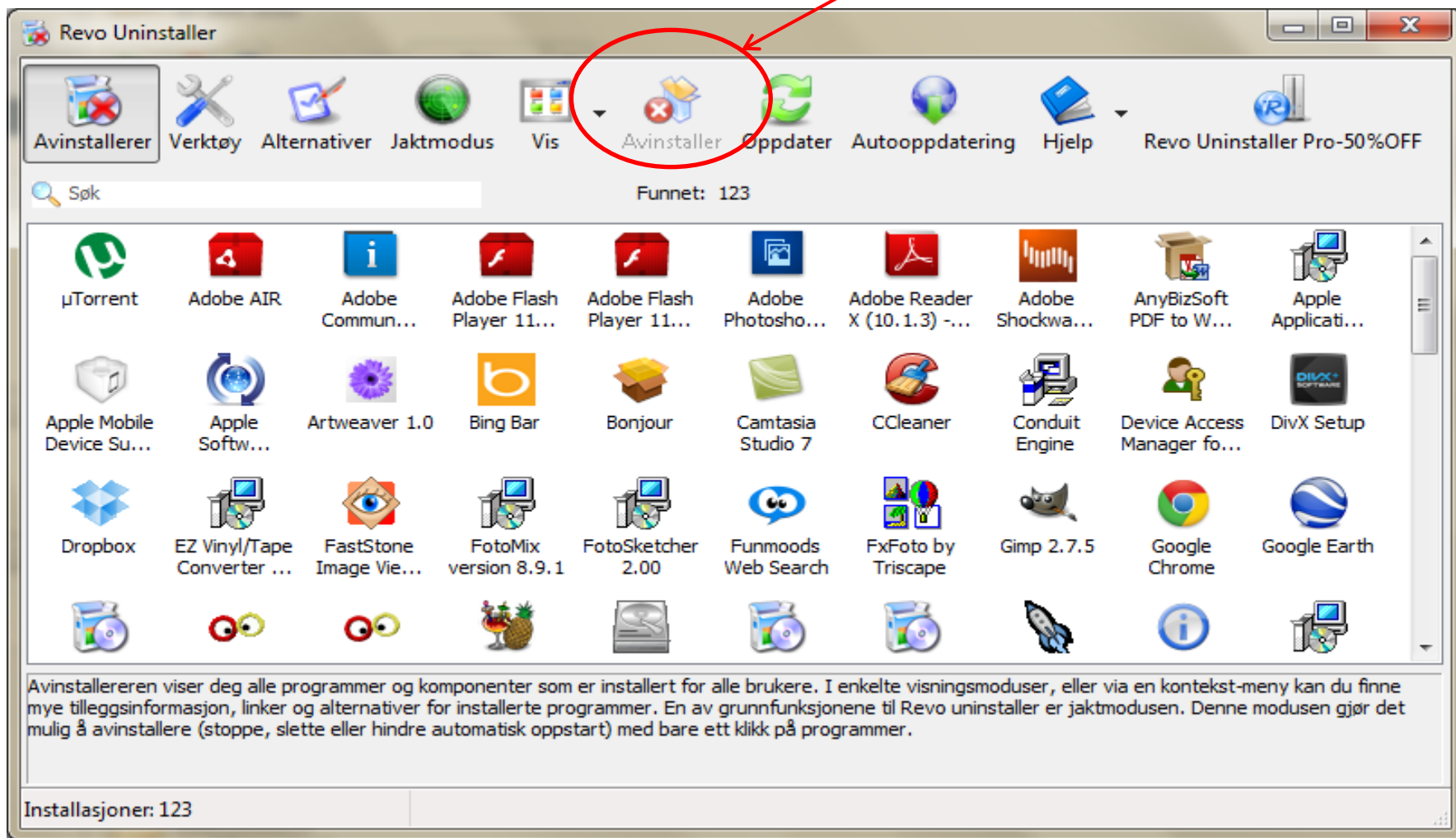
Revo Uninstaller  
Freeware Professional

Scanning for leftovers after the standard uninstall	FREE	FREE
Additional cleaning code included	FREE	FREE
Free Professional Technical Support	FREE	FREE
Extended scanning for leftovers - more advanced scanning algorithms	FREE	FREE
Real-Time monitoring of system changes - forcing install of programs	FREE	FREE
Forced Uninstall - remove remnants of already uninstalled programs	FREE	FREE
Multi-level Backup system - including full Registry backup	FREE	FREE
Print and Print Preview of installed programs	FREE	FREE
Export of installed programs - in TXT, HTML, and MS Excel	FREE	FREE
Compatible and flexible User Interface	FREE	FREE
Visual theme support	FREE	FREE
Compressed file program uninstall support	FREE	FREE
Full 64-bit compatibility - Windows XP, Windows Vista and Windows 7	FREE	FREE
Versional library	FREE	FREE
The Full Download of Revo Uninstaller	Download O.S.	Download O.S.

Revo Uninstaller Portable Download

For å kunne aktivisere nedlastingen må du scrolle litt ned på siden. Velg den Download-knappen som er markert på bildet. Dette er en permanent gratis versjon. Den ved siden av er bare en 30 dagers prøve (inntil man må betale for bruken)

- Etter du har lastet ned og startet programmet Revo, vil følgende bildet komme opp.
- Marker det programmet du vil avinstallere og trykk på «Avinstaller». Svar Ja på spørsmålet som dukker opp.  
Så vil bildet vist på neste siden komme frem.



- Velg her «Moderat» eller «Avansert» og trykk «Neste»  
Så vil avinstalleringen settes i gang. Følg så bare anvisninger.
- Dersom du ikke vil avinstallere trykker du «Avbryt»

