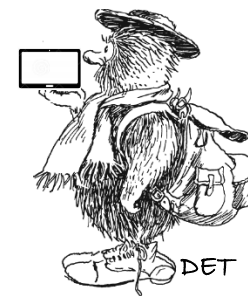


SIKKERHET PÅ NETT



DET ER FALG DET!!

Hva sikrer/låser vi?

- Hjemmet
- Nøkler til bilen
- Passord til datautstyr
>PC, Telefon, nettbrett
- Lås på postkasse
- Hoveddør og bakdør
- Hvor er nøklene?
- Hvem har tilgang?

Visste du at datamaskiner koblet til Internett angripes to ganger i minuttet?

Da er det greit å vite at finnes en rekke sikkerhetsprogram som gjør at du kan surfe og bruke nettet helt trygt.

Her er noen av farene din maskin kan utsettes for:

- Spionprogrammer som overvåker alt du gjør, stjeler identitetsinformasjon og eksempelvis tapper nettbanken din
- Din maskin brukes som e-postbase for virusinfisert e-post som sendes til tusenvis av e-postbrukere verden over
- Du besøker nettsteder som er en kopi av nettstedet du *tror* du besøker og angripes på ulikt vis (phising)
- Du besøker nettsteder som lurer deg til å laste ned og installere tilsynelatende uskyldig programvare som kan skade pc-en din eller inneholde spionprogrammer
- Maskinen din utsettes for ondskapsfulle angrep som resulterer i at hele eller deler av datamaskinens innhold slettes

OPPDATERING

HOLD OPERATIVSYSTEMET OPPDATERT

DET SAMME GJELDER FOR ALLE PROGRAMMER DU
BRUKER PÅ DIN PC, NETTBRETT OG SMARTTELEFON

Ha et antivirus program aktiv!

- Oppdateringer gjelder for alle programmer på din PC, men det er spesielt viktig for f.eks. ditt antivirus program
- Antivirusprogram bør også installeres på nettbrett og smarttelefon
- Mange antivirusprogrammer som Defender, har automatisk oppdatering. Sjekk hvordan det er for antivirusprogram du har på din PC. Åpne ditt antivirusprogram og fin valget for oppdatering.
- Gode gratis antivirus:
 - **Defender** – ligger som standard på Windows 8 og Windows 10. Fungerer bra for vanlig brukere av internett. Har blitt forbedret i den siste oppdatering av Windows 10.

Når en ønsker å installere en annen antivirus program, vil Defender automatisk deaktivere seg (den blir ikke borte men er ikke aktiv). Avinstallerer man det andre antivirus program vil Defender aktivere seg selv igjen. Dette gjelder altså for PC-er med Windows 8 eller 10. De med Windows 7 kan velge Microsoft Security Essentials eller en av de 3 programmer som står nedenfor.

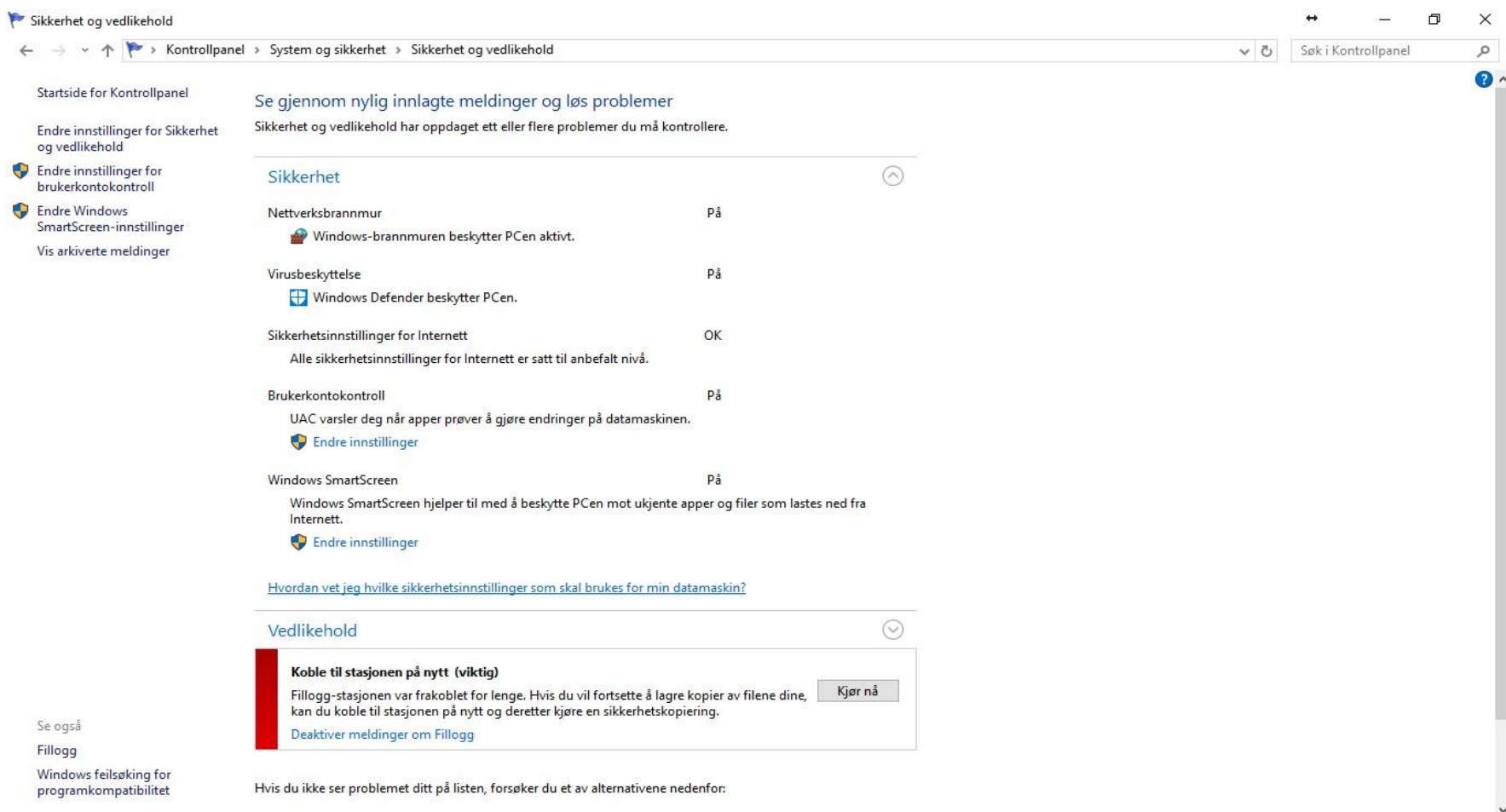
 - **Avast**
 - **Avira**
 - **AVG**
- Disse gratis antivirusprogrammer er minst like bra som de programmer en skal betale for (Norton, McAfee, F-secure m.fl.)

Ordforklaringer

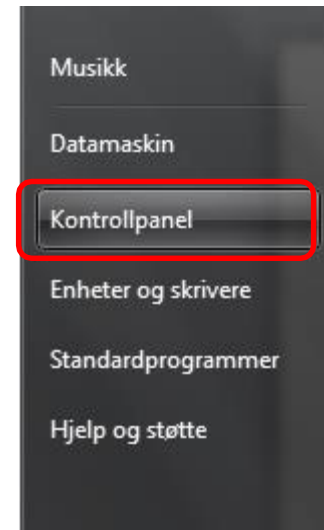
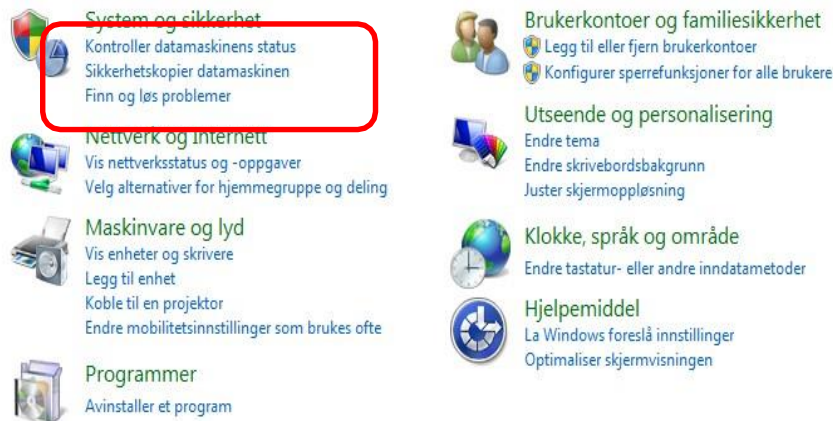
- **Et virus:** er en del av en datakode som knytter seg selv til et program eller en fil, slik at det kan spre seg fra datamaskin til datamaskin. Det infiserer mens det overføres. Virus kan ødelegge programvaren, maskinvaren og filene.
- **Orm:** en undergruppe av virus. En orm sprer seg generelt uten 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.
- **Phishing:** Engelsk ord for en form for internettbedrageri, som er basert på personlig informasjon. For eksempel etterligner kriminelle nettsiden til en pålitelig bank eller nettbutikk, og prøver å tiltrekke seg folk til dette nettstedet via e-post for så å få tak i opplysninger som brukes for å logge inn. Deretter kan de misbruke disse opplysninger.
- **Spam:** Engelsk ord for uønsket epost. Disse eposter inneholder ofte reklame for produkter eller nettsider. Spam utgjør så mye som 90 prosent av all e-post som sendes i verden (produkter, helse, finansielle tjenester).

Start Handlingssenter/Sikkerhetssenter i Kontrollpanel og kontroller sikkerhetsstatusen i Windows. Følg instruksjonene ved advarsler

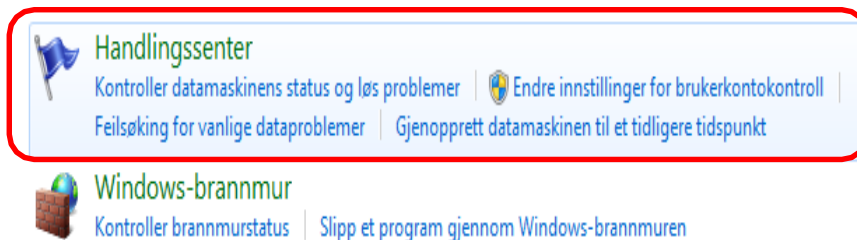
- Dersom du har Windows 10
 - Høyre klikk på Startknappen og velg Kontrollpanel
 - Velg System og Sikkerhet og deretter Sikkerhet og vedlikehold



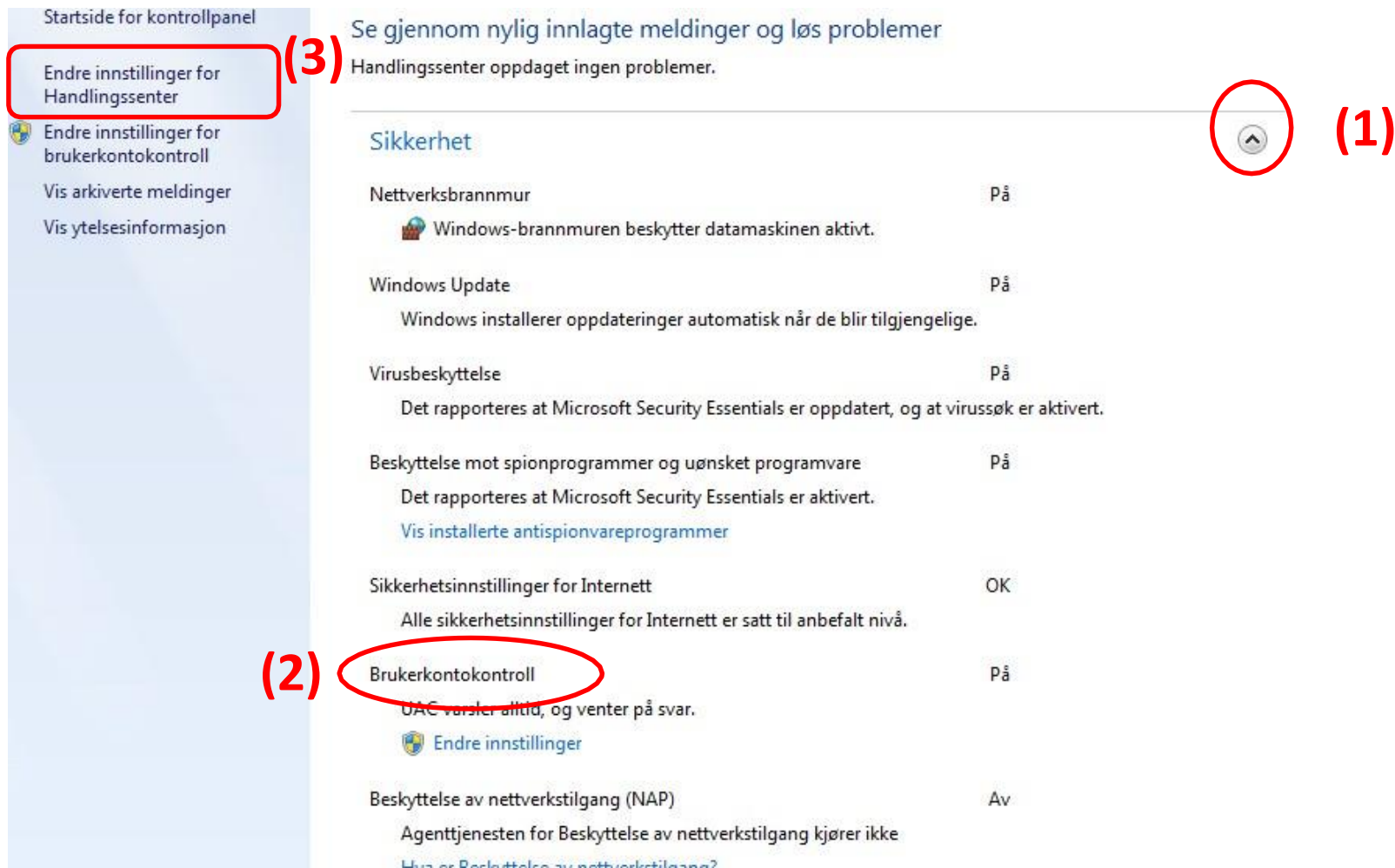
- Dersom du har **Windows 7**
- Klikk på «Startknappen»  og velg «Kontrollpanel»
- Kontrollpanel åpner med 8 kategorier og du velger kategori «System og Sikkerhet»



og deretter «Handlingssenter»



- 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)



The screenshot shows the Windows Security settings page. On the left, a sidebar contains links: 'Startside for kontrollpanel', 'Endre innstillinger for Handlingscenter' (highlighted with a red box and labeled (3)), 'Endre innstillinger for brukerkontroll', 'Vis arkiverte meldinger', and 'Vis ytelsesinformasjon'. The main area is titled 'Sikkerhet' and lists various security features with their status and a 'På' or 'Av' toggle. A red circle labeled (1) highlights the 'På' toggle for 'Sikkerhet'. Another red circle labeled (2) highlights the 'Brukerkontroll' entry. The 'Brukerkontroll' entry shows 'UAC venter alltid, og venter på svar.' and a link to 'Endre innstillinger'.

Sikkerhet	Status
Nettverksbrannmur	På
Windows Update	På
Virusbeskyttelse	På
Beskyttelse mot spionprogrammer og uønsket programvare	På
Sikkerhetsinnstillinger for Internett	OK
Brukerkontroll	På
Beskyttelse av nettverkstilgang (NAP)	Av

Passord

- Bruk passord som er en blanding av små og store tegn og som inneholder både tall, bokstaver og spesial tegn
- 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), tall og en eller flere spesial tegn (@, £, \$, € m.m.)
- Minst 8 tegn anbefales; hver ekstra karakter gjør det enda sterkere.
- Bruk aldri en hel rad av de samme tegnene på rad, for eksempel 55555 eller AAAAA, og pass på at passordet ikke er (deler av) brukernavnet eller vanlig navn.
- Ikke bruk kjente data av deg selv, for eksempel en fødselsdato
- Skifte av passord
 - Din leverandør er «hacket»
 - Etter du har gitt andre tilgang (f.eks. ved support)
- Forskjellige passord på forskjellige tjenester
 - Bank, NAV, Min helse, Digipost etc. (bankID)
 - Steder som lagrer kredittkortinformasjon
 - Epost som gmail, hotmail, online etc.
 - Felles for alle steder som er lite kritiske mht. personlig informasjon

- Dersom du vil ha hjelp til å lage passord, kan du bruke en passord generator (husk at slike program genererer passord som er veldig vanskelig å huske, men som er svært sikre).
Du finner en på <https://identitysafe.norton.com/no/password-generator#>
- Endre passord regelmessig på store nettsteder. Ved hjelp av phishing og spyware kan uautorisert personer få tilgang til passord. Svar aldri på forespørsler fra phishing e-post og sjekk maskinen regelmessig med et anti-malware program.
- 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
- Dersom en ønsker å bruke et såkalt Passordprogram (altså et program som husker alle dine passord) kan du bruke LastPass <https://lastpass.com/>

«Hovedregler» for bruk av elektronisk post

- Antivirus:
 - Windows 7 og 10 – Defender, Avast, Avira
 - Ipad/IOS - Avast, AVG, Norton etc.
 - Må oppdateres jevnlig
- Vær skeptisk ved mottak
 - Avsender mail@nav.no →
<mailto:mail@nav-svindel.no>
og er selvfølgelig svindelforsøk
 - Vedlegg
 - skal ikke åpnes med mindre du kjenner avsender og vet at han har sendt deg et vedlegg
- Svar
 - Ikke svar direkte på epost før avsender er sjekket
- Linker i teksten
 - ikke klikk på linker i epost, gå til nettleser og skriv/kopier inn linkene.
 - F.eks:
 - Link: <http://www.dnb.no/>
for det er:
<http://www.dnb-svindel.no/>
og er selvfølgelig svindelforsøk
- Epost fra venner og kjente?
 - Vær skeptisk hvis språket er utenlandsk og avsender skriver norsk til vanlig.
 - Vedlegg som virker «morsomme»
 - Sjekk gjerne med avsender om hva han/hun har sendt. Det kan være at avsender er infisert av virus

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. |

«Hovedregler» ved «surfing» - nettleserbruk

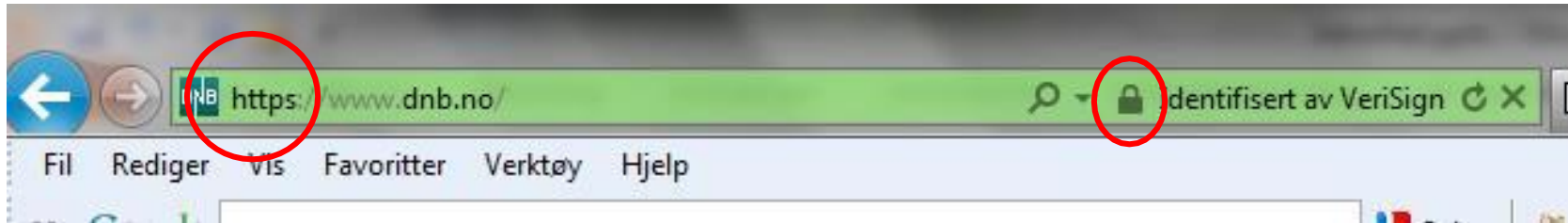
Nettlesere (eksempler): 1) er for Windows 2) er for IOS/Apple/Ipad

- Internet Explorer¹
 - Edge¹
 - Firefox¹⁺²
 - Chrome¹⁺²
 - Safari²
 - Det er mange flere ...
-
- Nettleser bør/må være oppdatert – eksempel:
 - Firefox (1 eksempel)
 - «Hjelp + om Firefox»
 - Vær kritisk til hva du surfer på; mer lugubre steder – større fare for å bli infisert
 - Sikre sider
 - <https://www.dnb.no/>
 - Usikre sider (lugubre)
 - Spill
 - Porno
 - Etc.
 - Usikker på hva det er? Søk på det! Dvs. bruk Google, og se hva du kan finne ut om det.

Se til at du bruker sikker nettside f.eks for nettbank

- Eksempelet her er nettbank fra DNB. Løsningen er noe 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.

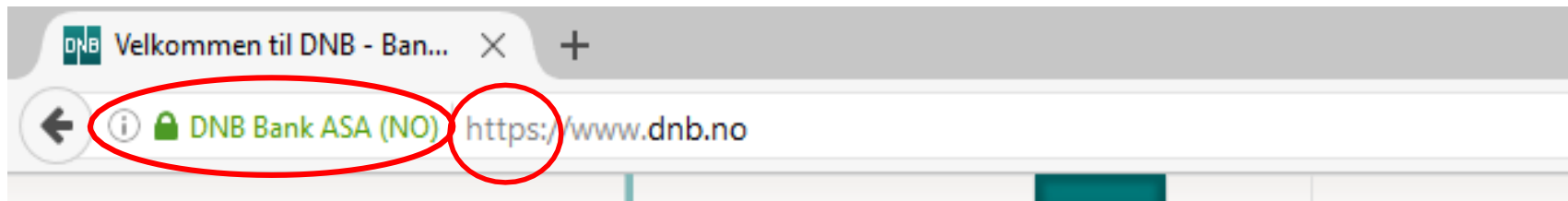
Slik vises det i Internet Explorer : hele adresselinje er grønn, https:// vises i adressen og du finner hengelåsen



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 er det VeriSign)



Slik vises det i Edge, Google Chrome og Firefox.



Både hengelås og DNB Bank ASA (NO) i grønn farge. Hengelps endrer ikke farge med når du klikker på den kommer meldingen om VeriSign frem. Også her vises https:// i adressen

Skylagring

- OneDrive
- Dropbox
- iCloud
- Box
- Osv. osv.
 - «Alle» tilbyr ekstern lagring
 - Fordel: - du kan nå dine bilder, dokumenter etc fra hvor som helst
 - Ulempe: - Hva vet man om hvor dataene er? Hvordan er sikkerheten?
- Alternativ til dette er sikkerhetskopiering hjemme på f.eks. en ekstern harddisk
 - Denne sikkerhetskopi bør ligge på et trygt sted f.eks. i brannsikkert skap
 - Tas kopi ofte nok?

Trygg netthandel

- **Falske nettbutikker**

Falske nettbutikker har gjerne ett av to mål: å lure til seg penger eller å lure til seg sensitiv informasjon de kan bruke til å gjennomføre ID-tyveri, sånn at de kan lure til seg penger.

Hva kan man se etter?

- **Ingen eller mangelfull kontaktinfo** - I følge angrerettloven er alle norske nettbutikker pålagt å oppgi organisasjonsnummer, geografisk adresse, e-postadresse og en enkel måte å kontakte kundeservice på, enten et telefonnummer eller en chattetjeneste.
- **Prisene er veldig reduserte** - det hender varer er på tilbud, men sjelden til mange 1000 kr billigere enn normalt. Sammenlign prisene med andre nettbutikker før du kjøper noe, forskjellen bør ikke være for stor.
- **Dårlig språk** - De fleste falske nettbutikker er ikke norske, og selv om all informasjonen er skrevet på norsk betyr ikke det at butikken nødvendigvis er norsk. Med automatiske oversettingstjenester er det lett for svindlere å lage en norsk nettside. Men det er ofte lett å avsløre at tekst er automatisk oversatt. Setningene er ofte preget av dårlig grammatikk og setningsoppbygging, ord som ikke gir mening i konteksten og av og til tilfeldige ord på et helt annet språk.
- **Rare nettadresser** - seriøse nettbutikker har sjelden navn som inneholder ord som billig, cheap, salg, tilbud og lignende. Man bør også være obs på nettadresser som inneholder merkenavn, og spesielt hvis det er kombinert med ord som billig også videre. Eksempler: www.billigburberry.com, www.billignikefreerunsko-norge.com, www.cheapfreeonsale.org.
- **Nettadresser og butikknavn som ikke stemmer overens** - ofte nettbutikken heter noe annet enn hva nettbutikken heter, det er fordi svindlerne ofte beholder den samme nettadressen og tilpasser siden til hvilke merkevarer som er etterspurt, og fordi produsenten av de ekte merkevarene gjerne eier nettadressene med merkenavnet i. Eksempel: en butikk har nettadressen www.jakkesalg.eu mens det inne på nettsiden står at den heter Canada Goose Norge.
- **Dårlig kvalitet** - Fordi svindlerne regner med at mange nok ukritisk lar seg lokke av de gode tilbudene til at de kan tjene gode penger, er sidene ofte preget av dårlig kvalitet. Dette synes blant annet gjennom at lenker og knapper ikke virker og informasjon ikke stemmer overens, eller mangler helt.
- **Forbrukerombudets liste over falske nettbutikker:** www.forbrukerombudet.no/netthandel/falske-nettbutikker
- **Bruk Google:** søk på Google om andre har skrevet noe om denne nettsiden

Sikker betaling ved netthandel

- En generell regel på internett er at man aldri skal dele sensitiv informasjon med noen, med sensitiv informasjon menes kontonummer, kortnummer, sikkerhetskode (CVC), passord, pinkoder, personnummer også videre. Kort sagt all informasjon noen kan bruke til å få tilgang til dine brukerkontoer eller personopplysninger. Sensitiv informasjon på avveie kan føre til ID-tyveri og store pengetap.
- **Hvilken informasjon skal jeg gi fra meg?**
- **Personnummer:** Nettbutikker har i utgangspunktet ikke lov til å be om personnummer, unntaket er hvis de skal gjennomføre en kredittsjekk ved opprettelse av mobilabonnement, betalingsavtaler og lignende. Oppgi derfor aldri personnummer hvis du ikke kjøper en tjeneste der kredittsjekk er nødvendig.
- **Kontonummer:** Det er ikke mulig å hente ut penger fra en bankkonto kun med et kontonummer, det er derfor heller ingen grunn for nettbutikker å be om det. Jo mer informasjon svindlere klarer å samle, jo lettere er det å gjennomføre ID-tyveri. Hvis du selger varer gjennom for eksempel FINN.no anbefales det å bruke andre, sikrere betalingsløsninger.
- **Kortinformasjon:** med mindre man betaler med faktura kommer man ikke unna å oppgi kortinformasjon, hvis man bruker en sikker betalingsløsning går det fint.
- **E-postadresse, postadresse og telefonnummer:** Når man handler på nett må man alltid oppgi e-postadresse og postadresse. E-postadressen brukes til å sende kvitteringer og annen kommunikasjon, og for å opprette en brukerkonto hvis det er ønskelig. Postadressen må man oppgi for å motta varen. Om du må oppgi telefonnummer varierer mellom butikker, hos noen er det valgfritt, hos andre obligatorisk.

- **Betaling**

- Det finnes mange måter å betale for seg på nett, noen anbefales sterkt og andre bør unngås til en hver pris.

- **Anbefalt! Kredittkort:** Kredittkort er betalingsmåten bankene anbefaler. Hvis du betaler med kredittkort kan du ha rett på tilbakebetaling av pengene dersom du skulle være uheldig å oppleve svindel eller at firmaet går konkurs. For å få innvilget tilbakebetaling må man ha kontaktet selgeren først og ta kontakt med banken innen rimelig tid. Tilbakebetalingsretten gjelder ikke hvis man handler fra en privatperson. Hvis du kjøper en reise og betaler over 50% av reisen med kredittkort får du også reiseforsikring.
- **Debetkort:** Debetkort har ikke de samme rettighetene som betaling med kredittkort, med debetkort har du ikke rett på tilbakebetaling.

- **Kontooverføring:** Med overføring direkte til konto har du ingen rettigheter til tilbakebetaling om det skulle skulle skje noe.

- **Faktura:** Fordelen med faktura er at du ikke trenger å forhåndsbetale, men et fakturagebyr vil som regel påløpe. Med faktura har man 14 dagers betalingsfrist.

- **PayPal:** Paypal er en amerikansk tjeneste som tilbyr overføring av penger vi internett. Tjenesten brukes av både bedrifter og privatpersoner for enkel betaling. Om det skulle oppstå problemer i salgsprosessen er PayPal behjelpelige med å løse problemet og kan stoppe utbetalinger til selger. Dette er tjenesten som oftest anbefales når det kommer til kjøp og salg mellom privatpersoner.

- **Western Union:** Western Union tilbyr overføring av penger internasjonalt, og har kontorer i hele verden. Men tjenesten er yndet av svindlere fordi sikkerheten er relativt lav. Det er ikke vanskelig å hente ut penger med falsk ID, og noen plasser i verden trenger man ikke ID i det hele tatt. Det anbefales derfor ikke å betale for kjøp gjennom Western Union:

- **Sjekk:** Det finnes mange tilfeller av svindlere som ønsker å betale for varer på for eksempel FINN.no med sjekk. Det anbefales på det sterkeste å ikke ta i mot sjekk da disse ofte er falske (Det er også dyrt å sjekker, 450 kr hos DNB og NORDEA).

- **Sikker betaling:** disse betalingsløsningene er alle sikre i bruk, hvilke som er tilgjengelige avhenger av nettbutikkens avtaler, men alle har høye krav til sine samarbeidspartnere. Nettbutikker med en eller flere av disse løsningene er derfor som oftest til å stole på.
- **FINN Trygg betaling:** Dette er en tjeneste FINN.no tilbyr brukere av sine tjenester. I stedet for at kjøper betaler direkte til segler betaler han inn til FINN, FINN gir beskjed til selgeren om at pengene er mottatt og selgeren sender varen. Når kjøper mottar varen og har sjekket at alt er i orden gir han beskjed til FINN og FINN utbetaler pengene til selgeren. På denne måten hindrer man at noen betaler på forskudd for en vare som ikke kommer eller at man sender fra seg en vare man aldri får betalt for.
- **3D Secure:** 3D Secure er en tjeneste de fleste norske, og mange internasjonale butikker benytter seg av i dag. Betaler du med VISA eller MasterCard i en nettbutikk som bruker 3D Secure vil du bli bedt om et passord. Som oftest er dette BankID, men noen ganger er det en engangskode sendt på SMS eller et bestemt passord, avhengig av hvilken kortutsender du har.
- **Klarna og PayEx:** klarna og PayEx er selskaper som behandler betalingsprosessen for nettbutikker. De tilbyr blant annet betaling med kreditt- og debetkort, faktura og delbetaling. Disse firmaene har høye krav for nettbutikkene de samarbeider med, og er derfor veldig sikre i bruk. Skulle det oppstå problemer kan de hjelpe deg med å løse det.
- **Lagring av kredittkortinformasjon:** Det finnes mange tjenester som kan lagre kredittkortinformasjonen din for å gjøre det lettere for deg å handle. Dette er en tjeneste som tilbys av både nettlesere og nettbutikker. I nettleserne og seriøse nettbutikker lagres denne informasjonen kryptert, det vil si at det i utgangspunktet er trygt å lagre, men om passordet ditt skulle havne på avveie vil det være mulig for uvedkommende å få tilgang til kortinformasjonen din
- **Viktig! Sjekk om nettsiden er kryptert:** Før du fører inn noe som helst informasjon på en nettside må du sjekke at siden er kryptert. Det vil si at informasjonen som førest inn på siden blir kodet om slik at uvedkommende ikke kan lese den. Om en nettside er kryptert ser du i adressefeltet. Helt til venstre i feltet skal det være et hengelås, i noen nettlesere står det "Sikker" ved siden av hengelåsen, og nettadressen skal begynne på https:// (ikke http://)

Hvordan kan du sjekke om en nettside inneholder virus?

Nettside: <https://www.virustotal.com/nb/>

Trykk på fanen Nettsadresse – kopier nettsadressen (URL) du vil kontrollere – lim inn URL i det tome feltet – trykk på Scan



VirusTotal er en gratis tjeneste som **analyserer mistenkelige filer og URLer** og tilrettelegger for rask deteksjon av virus, ormer, trojanere og alle typer malware.

 Fil

 Nettsadresse

 Søk

<http://www.example.com/>

Skriv inn URL

Scan!

Resultatet fra Scan av nettsiden til Seniornett (siste analyse 01.08.2017) viser en deteksjonsrate 0/65 som betyr 0 feil oppdaget fra test av 65 antivirusprogrammer.

URL: <https://www.seniornett.no/>

Deteksjonsrate: 0 / 65

Analysedato: 2017-08-01 13:28:21 UTC (4 uker siden)

HELST IKKE BRUK ET ÅPENT TRÅDLØS NETTVERK

- **Ikke bruk usikre nettverk:** hold deg til sikre nettverk eller mobildata. Nå tilbyr alle mobilskoper bruk av mobildata i EU til samme pris som hjemme, dermed er mobildata et godt alternativ selv om du er på ferie.
- **Aldri bruk nettbank eller betal med kort på ukjente nettverk:** det er spesielt viktig å verne om bankinformasjonen din, slik at uvedkommende ikke får tilgang til dine penger. Unngå derfor å oppgi denne informasjonen når du bruker usikrede nettverk.
- **Logg deg av alle brukerkontoer når du ikke bruker de:** Av og til kan hackere få tilgang til brukerkontoene dine, som for eksempel Facebook og e-post, uten passord. Alt de trenger er at du er pålogget. Logger du deg av når du ikke lenger bruker den, kan du forhindre dette.
- **Skrur av WiFi på enheten din når du ikke bruker det:** Hvis du skruer av WiFi når du ikke bruker det, unngår du at du kobler deg til nettverk uten at du vet om det selv. Som en bonus sparer du også strøm.
- **Ikke stol på nettverket bare fordi du stoler på eieren:** I de aller fleste tilfeller er det ikke eieren av nettverket som er ute etter å hacke, så ikke stol på at nettverket er trygt bare fordi du stoler på eieren.

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

Spam: Sjøppelpost brukes som betegnelse på uønsket reklame og annen masseutsendt informasjon som ikke er godkjent av mottakeren. Begrepet brukes hovedsakelig om uønsket masseutsendt e-post.

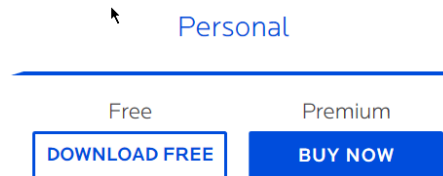
- Åpne bare e-post fra de du kjenner
- Åpne bare vedlegg du stoler på eller vedlegg som virker logisk og har et logisk navn
- E-posten virker mistenkelig selv om den er sendt av en du kjenner. Det er mistenkelig når emne eller vedlegget:
 - har et langt navn med mange bokstaver og tall blandet
 - har 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).

Installer tilleggsprogrammer for ekstra sikkerhet som Antimalware og Antispyware

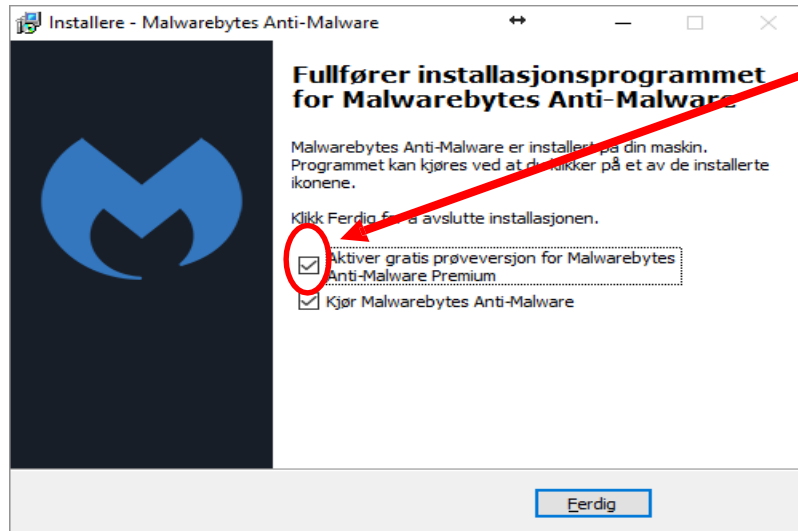
- Antimalware program kan du laste ned gratis fra Malwarebyte

<https://www.malwarebytes.com/mwb-download/>

- Velg Download free



Dersom dette bilde vises på slutten av installeringen (ikke sannsynlig men kan skje):



Ta vekk hake foran «Aktiver gratis prøveversjon for.....»

Etter at programmet har startet trykker du på Skann nå. Den skanningen kan ta litt tid. Dersom det etter skanningen er funnet feil, trykk på "Fjern feil" og vent til Ferdig

- Antispyware program kan du laste ned gratis fra

www.superantispyware.com/

Når du kommer til nettsiden, klikk på «Free Edition Download»

Klikk deretter på «Kjør» og følg anvisninger på skjermen

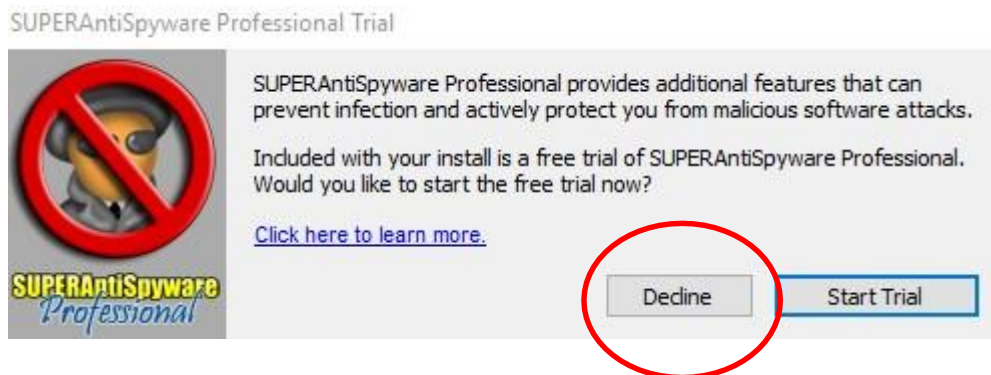
Alt etter hvilken nettleser man bruker, trykker du på Kjør (IE og Edge) eller Lagre (Firefox) eller direkte på nedlastingen nederst til venstre (Chrome).

Følg så anvisningen på skjermen

OBS!! På slutten kommer dette bilde.

Ikke trykk Enter men klikk på «Decline»

Velger man «Start Trial» har man tatt i bruk betal versjonen av programmet!!



Installer program for sikker avinstallering og for rensing av harddisk

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/revo_uninstaller_free_download.html

For å kunne aktivisere nedlastingen må du scrolle (rulle) litt ned på siden til du kommer til Revo Uninstaller Freeware og trykk på den Free Download-knappen som er markert på bildet.

The screenshot shows the website for Revo Uninstaller Freeware. The title 'Revo Uninstaller Freeware' is circled in red. A red arrow points from the text 'Revo Uninstaller Freeware' in the paragraph above to this title. Another red arrow points from the text 'trykk på den Free Download-knappen' in the paragraph above to a blue button labeled 'FREE DOWNLOAD'. Below the title, there are three features listed with checkmarks: 'Scanning for leftovers after the standard uninstall', '8 Additional cleaning tools included', and 'Free Professional Technical Support'. Below the 'FREE DOWNLOAD' button is a yellow button labeled 'COMPARE PRODUCTS'. At the bottom right, the version 'Version: 2.0.1' is displayed, followed by a paragraph stating that the software is compatible with various Windows versions.

Revo Uninstaller Freeware

- ✓ Scanning for leftovers after the standard uninstall
- ✓ 8 Additional cleaning tools included
- ✓ Free Professional Technical Support

FREE DOWNLOAD

COMPARE PRODUCTS

Version: 2.0.1

Revo Uninstaller Free is fully compatible with 32-bit and 64-bit versions of Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 and Windows Server

- 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.

Revo Uninstaller 2.0.1

Avinstallerer

Verktøy

Jaktmodus

Alternativ

Avinstallere

Oppdatere programlisten

Vis

Hjelp

Upgrade to Pro-50%OFF

Søk etter:
Navn

Program	Størrelse	Versjon	Type	Installeringsdato	Firma	Webside	Kommentar
Adobe Acrobat Reader DC - Norsk	411,48 MB	15.020.20039	32-bit	14.10.2016	Adobe Systems Incorpara...	http://www.adobe.com/...	
Adobe Creative Cloud	239,97 MB	3.8.0.310	32-bit	28.09.2016	Adobe Systems Incorpara...		
Adobe Flash Player 23 NPAPI	5,90 MB	23.0.0.185	32-bit	14.10.2016	Adobe Systems Incorpara...	http://www.adobe.com/...	
Adobe Photoshop CC 2015.5	1,21 GB	17.0.1	32-bit	30.09.2016	Adobe Systems Incorpara...	http://www.adobe.com/...	
Adobe Photoshop CS6	116,21 MB	13.0	32-bit	14.10.2016	Adobe Systems Incorpara...		
Apple Software Update	4,81 MB	2.1.4.131	32-bit	04.08.2016	Apple Inc.	http://www.apple.com/n...	
Apple-programvaresupport (32-bits)	170,49 MB	4.1	32-bit	24.10.2016	Apple Inc.	http://www.apple.com/n...	
Apple-programvaresupport (64-bits)	188,09 MB	4.1	64-bit	24.10.2016	Apple Inc.	http://www.apple.com/n...	
ASUS GIFTBOX Desktop	3,54 MB	1.1.5	32-bit	04.08.2016	ASUS	http://support.asus.com	ASUS GIFTBOX Desktop
ASUS HiPost	20,57 MB	1.0.6	32-bit	04.08.2016	ASUS		
ASUS Live Update	11,71 MB	3.4.3	32-bit	06.09.2016	ASUS	http://support.asus.com/	An utility to support upgr...
ASUS Smart Gesture	121,72 MB	4.0.5	32-bit	04.08.2016	ASUS	http://support.asus.com/	
ASUS Splendid Video Enhancement Technology	46,58 MB	3.13.0004	32-bit	04.08.2016	ASUS		
ASUS USB Charger Plus	18,04 MB	1.1.6	32-bit	04.08.2016	ASUS	http://support.asus.com/	An utility to support quic...

Forklaringspanel

Avinstallering viser alle de programmer og komponenter som er installert til alle brukere. I detaljvisning, eller via høyreklikk, kan du finne mer informasjon (links og egenskaper). En av de primære funksjoner i Revo Uninstaller er jaktmodus. Denne metode gjør det mulig å avinstallere, stoppe, slette eller hindre automatisk oppstart med et enkelt klikk.

Installerte: 105

lysilde 16 av 17

Norsk (bokmål)

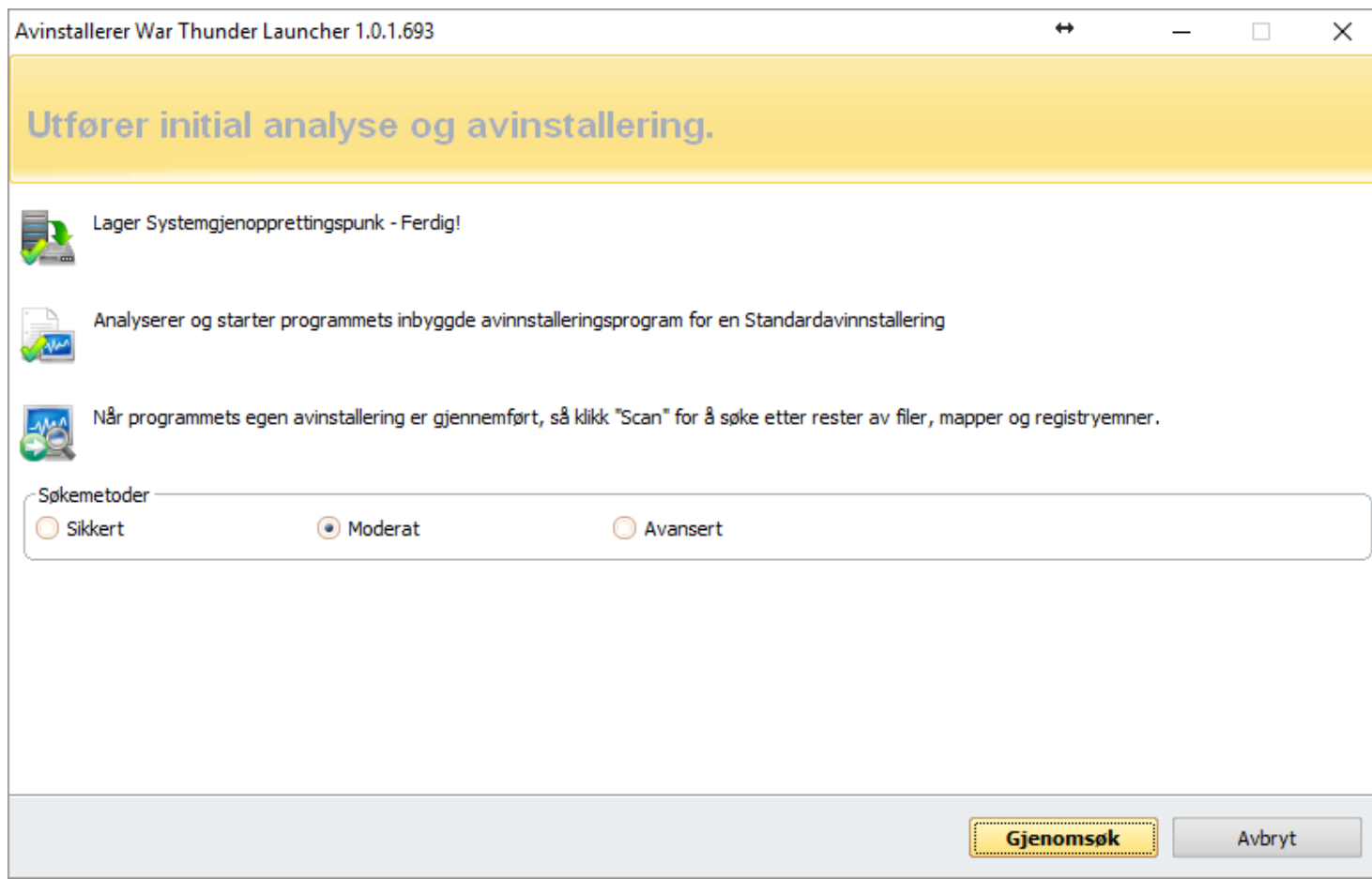
Notater

Kommentarer

Activate Revo Uninstaller Pro

Like us

- Programmet avinstalleres nå.
- Etter dette må maskinen gjennomføres om det fortsatt ligger (skjulte) filer, som tilhører programmet du har avinstallert, igjen på din PC. La valget stå på Moderat og trykk Gjennomøk.
- Dersom det finnes fortsatt filer på din PC som tilhører programmet, vil disse komme fram. Slett disse ved å følge anvisninger.



Et gratis program for rensing av harddisk er CCleaner.

- Last ned CCleaner fra <https://www.piriform.com/ccleaner/download>
- Dette vinduet kommer frem. Velg nedenfor CCleaner Free knappen Download

	 CCleaner Free	 CCleaner Professional	 CCleaner Professional Plus
Faster Computer	✓	✓	✓
Privacy Protection	✓	✓	✓
Complete Cleaning	✗	✓	✓
Real-time Junk Monitoring	✗	✓	✓
Automatic History Cleaning	✗	✓	✓
Automatic Updating	Manual	✓	✓
Defragmentation			✓
File Recovery			✓
Hardware Analysis			✓
		  €19.95	 €39.95 €69.95

- Etter at CCleaner er lastet ned og har startet ser man dette programmet
- I utgangspunktet kan alle valg som er huket av stå som de står. Men du kan f.eks. ta vekk hake foran «Sist brukte dokumenter» under Windows Explorer
- Klikk på «Kjør CCleaner» og velg OK i vinduet som kommer opp.

