

# Trygg på Internett

Hva bør vi vite sikkerhet på nettet?



# 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.
- **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).

## 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

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.

# OPPDATERING

HOLD TIL EN HVER TID OPERATIVSYSTEMET  
OPPDATERT

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

# Ha et antivirus program aktiv!

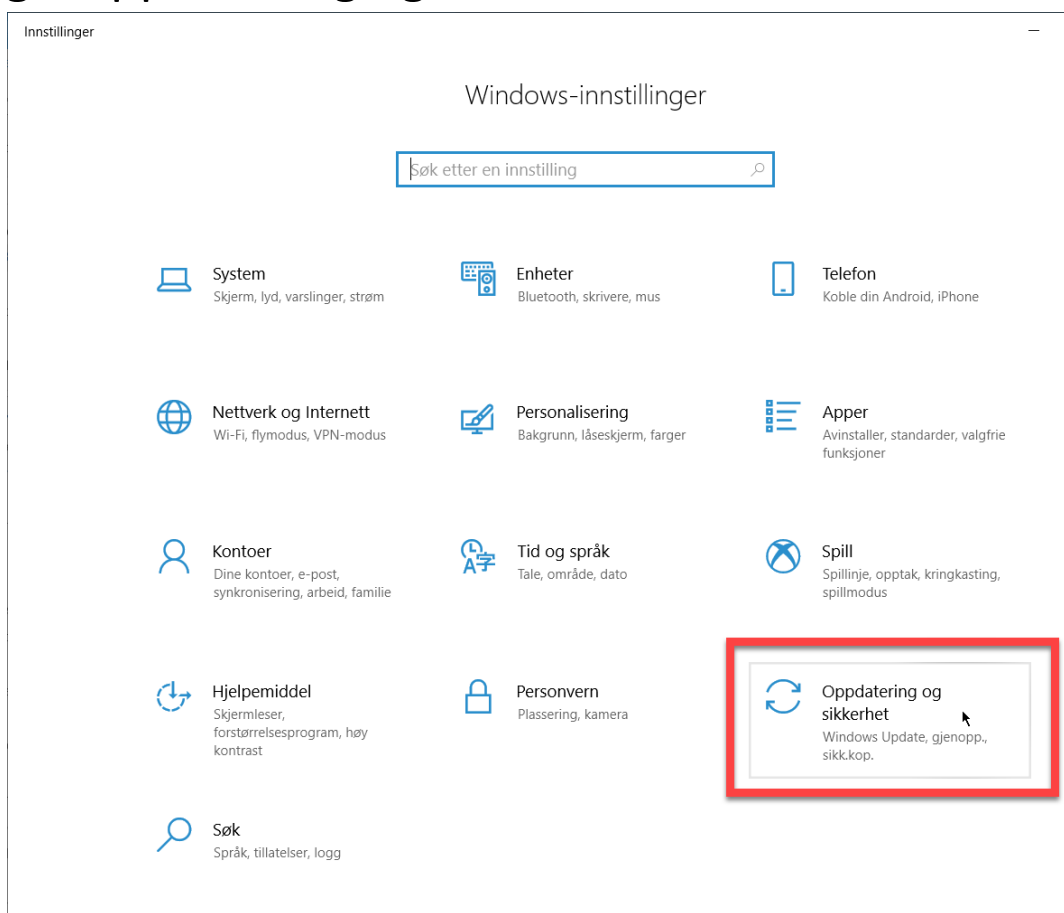
- Oppdateringer gjelder for alle programmer på din PC, men det er spesielt viktig for f.eks. ditt antivirus program
- Antivirusprogram bør også installeres på nettbrett og smarttelefon
- Mange antivirusprogrammer som Defender, har automatisk oppdatering. Sjekk hvordan det er for antivirusprogram du har på din PC. Åpne ditt antivirusprogram og fin valget for oppdatering.
- Gode gratis antivirus:
  - **Defender** – ligger som standard på Windows 10. Fungerer meget bra for vanlig brukere av internett. Blir stadig bedre med hver 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, Kaspersky m.fl.)

# Kontrollere om sikkerheten er i orden på din PC

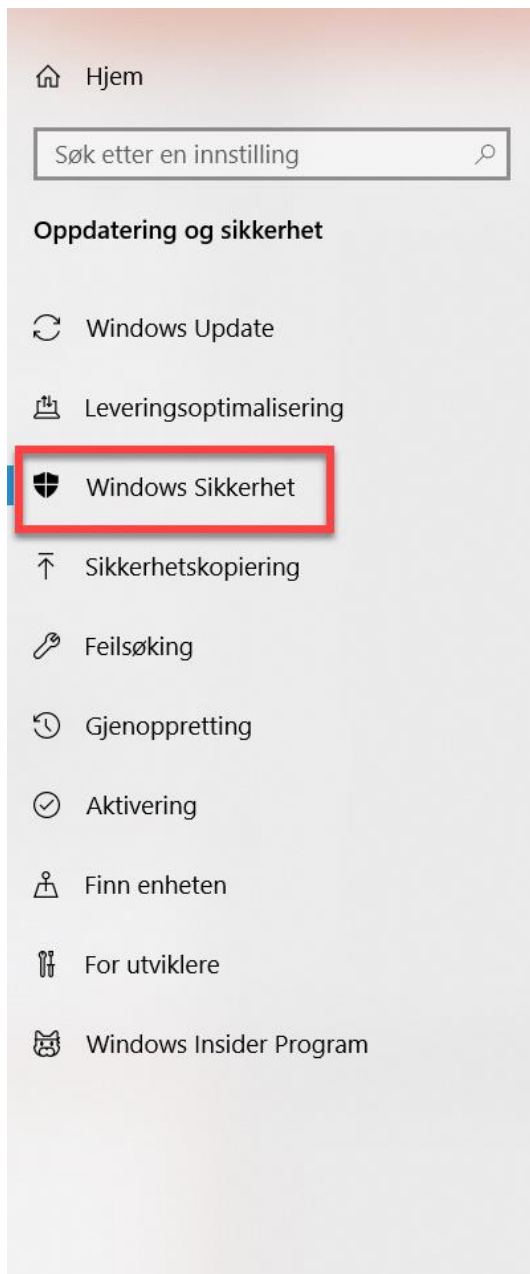
Trykk på Startknappen (1) og deretter på Innstillinger («») (tannhjulet)



Velg «Oppdatering og sikkerhet»



# Trykk på «Windows Sikkerhet» og velg deretter «Åpne Windows Sikkerhet










## Windows Sikkerhet

Windows Sikkerhet er hjemmet ditt for å vise og administrere sikkerheten og tilstanden til enheten din.

Åpne Windows Sikkerhet

### Beskyttelsesområder


-  Virus- og trusselbeskyttelse  
Krever ingen handlinger.
-  Kontobeskyttelse  
Krever ingen handlinger.
-  Brannmur og nettverksbeskyttelse  
Krever ingen handlinger.
-  App- og leserkontroll  
Krever ingen handlinger.
-  Enhetsikkerhet  
Krever ingen handlinger.
-  Enhetsytelse og -tilstand  
Handlinger anbefales.
-  Familiealternativer  
Administrer hvordan familien bruker enhetene sine.




### Beskytt PC-en din

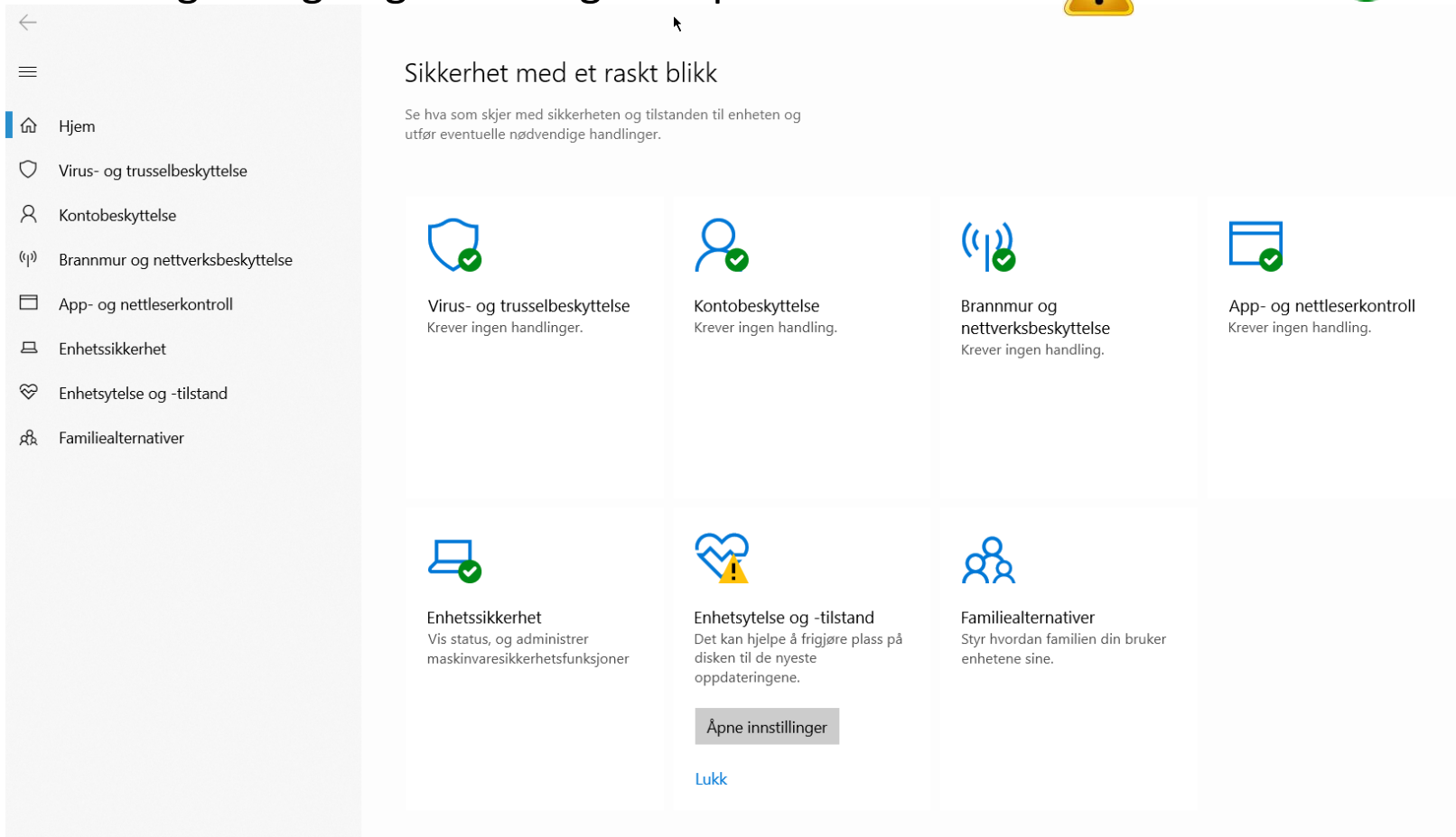
Windows Sikkerhet hjelper deg å være beskyttet på nettet, holde enheten i god stand, kjøre skanninger med jevne mellomrom, administrere innstillingene for beskyttelse mot trusler og mer.

[Få mer informasjon om Windows Sikkerhet](#)



I oversikten som kommer frem får man en rask oversikt over sikkerheten på PC-en, som om det et aktivert antivirusprogram, om brannmuren er på osv. Dersom det er OK vil det vises med en 

Dersom programmet oppdager et problem, vil det vises som en varseltekant  som her i «Enhetsytelse og -tilstand». Dersom det vises en varseltekant vil det som regel også vises et forslag til løsning. I dette tilfelle: trykk på «Åpne Innstillinger» og følg anvisninger. Er problemet løst vil  endres til 



The screenshot shows the Windows Security application interface. On the left is a navigation sidebar with the following items: Hjem, Virus- og trusselbeskyttelse, Kontobeskyttelse, Brannmur og nettverksbeskyttelse, App- og nettleserkontroll, Enhetsikkerhet, Enhetsytelse og -tilstand, and Familiealternativer. The main content area is titled "Sikkerhet med et raskt blikk" and includes a subtitle: "Se hva som skjer med sikkerheten og tilstanden til enheten og utfør eventuelle nødvendige handlinger." Below this are seven status tiles arranged in two rows. The top row contains: "Virus- og trusselbeskyttelse" (green checkmark), "Kontobeskyttelse" (green checkmark), "Brannmur og nettverksbeskyttelse" (green checkmark), and "App- og nettleserkontroll" (green checkmark). The bottom row contains: "Enhetsikkerhet" (green checkmark), "Enhetsytelse og -tilstand" (yellow warning triangle), and "Familiealternativer" (no icon). The "Enhetsytelse og -tilstand" tile has a button labeled "Åpne innstillinger" and a link "Lukk" below it.

Category	Status	Action
Virus- og trusselbeskyttelse	OK (Green checkmark)	Krever ingen handlinger.
Kontobeskyttelse	OK (Green checkmark)	Krever ingen handling.
Brannmur og nettverksbeskyttelse	OK (Green checkmark)	Krever ingen handling.
App- og nettleserkontroll	OK (Green checkmark)	Krever ingen handling.
Enhetsikkerhet	OK (Green checkmark)	Vis status, og administrer maskinvarerikkerhetsfunksjoner
Enhetsytelse og -tilstand	Warning (Yellow triangle)	Det kan hjelpe å frigjøre plass på disken til de nyeste oppdateringene. <a href="#">Åpne innstillinger</a> <a href="#">Lukk</a>
Familiealternativer	OK (No icon)	Styr hvordan familien din bruker enhetene sine.

# 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.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.
- Banker og seriøse bedrifter vil **ALDRI** sende deg slike typer e-post.

Nedenfor vises 3 eksempler av e-poster som er mistenkelige, og som prøver å lure deg.

Kære kunde Nordea

Du har 1 New Security besked!

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

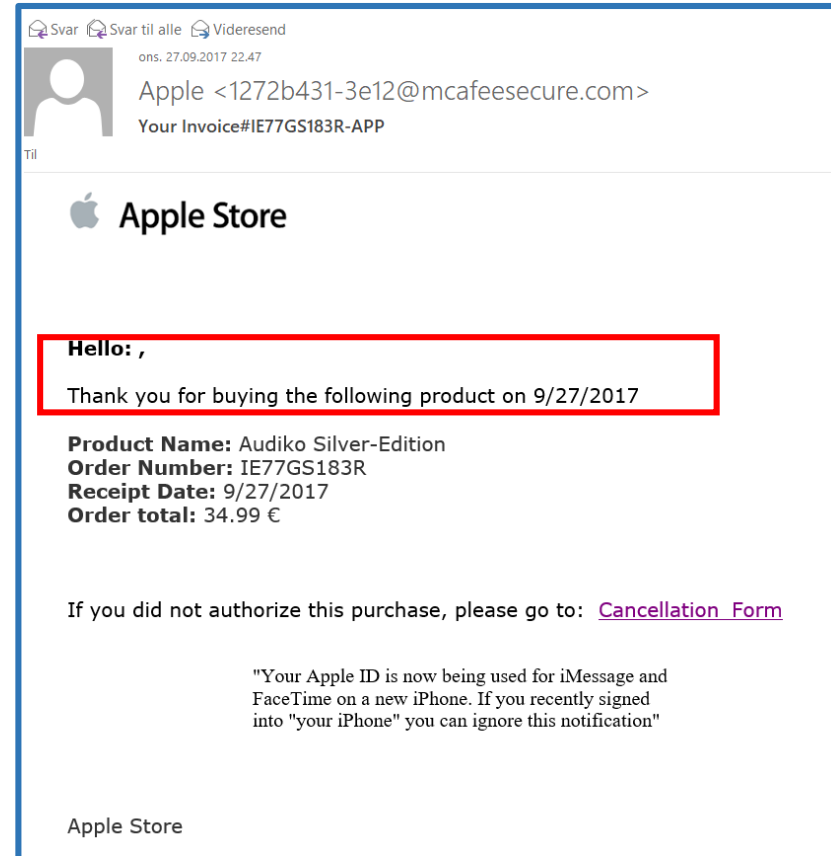
[Klik her for at løse problemet](#)

Takk for at du bruker SpareBank 1

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

## **Kommentarer:**

Banken vil **ALDRI** sende ut slike eposter.  
Dette er svindel. Slett slike eposter



## **Kommentarer:**

Det som kommer tilsynelatende fra Apple viser seg å ha blitt sendt av en robot (mange tall og bokstaver foran @) uten noen som helst henvisning til Apple. Svindel altså! Slett eposten!

Hello!

My nickname in darknet is linoel60.

I hacked this mailbox more than six months ago, through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

If you don't believe me please check 'from address' in your header, you will see that I sent you an email from your mailbox.

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.

Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

I was most struck by the intimate content sites that you occasionally visit.

You have a very wild imagination, I tell you!

I

During your pastime and entertainment there, I took screenshot through the camera of your device, synchronizing with what you are watching.

Oh my god! You are so funny and excited!

I think that you do not want all your contacts to get these files, right?

If you are of the same opinion, then I think that \$588 is quite a fair price to destroy the dirt I created.

Send the above amount on my BTC wallet (bitcoin): 19D67Tgb3neJiThd8pZDEBYmUn2qSjxEeB

As soon as the above amount is received, I guarantee that the data will be deleted, I do not need it.

Otherwise, these files and history of visiting sites will get all your contacts from your device.

Also, I'll send to everyone your contact access to your email and access logs, I have carefully saved it!

Since reading this letter you have 50 hours!

### **Kommentarer:**

*Dette er også svindel. Det er ingenting i denne eposten som virkelig viser til at din epost er «hacked». Her spiller, den som sender dette, på frykt og på uvitenhet av epost mottakeren. Slett slike eposter umiddelbart.*

# Sikkerhet i sosiale medier.



## Kommentarer:

- Dette er en klassisk fremgangsmåte fra svindlere på nettet. Her spilles det på **fristelse** (kan enkelt løse problemet), **frykt** (skremmende med virus) og **tillit** (meldingen ble sendt av en venn)
- Brukernavn og passord vil ikke bli brukt for å fjerne "viruset", men vil bli sendt til svindleren som driver nettstedet som så får tilgang til offerets brukerkonto for den valgte tjenesten.

# «Hovedregler» ved «surfing» - nettleserbruk

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

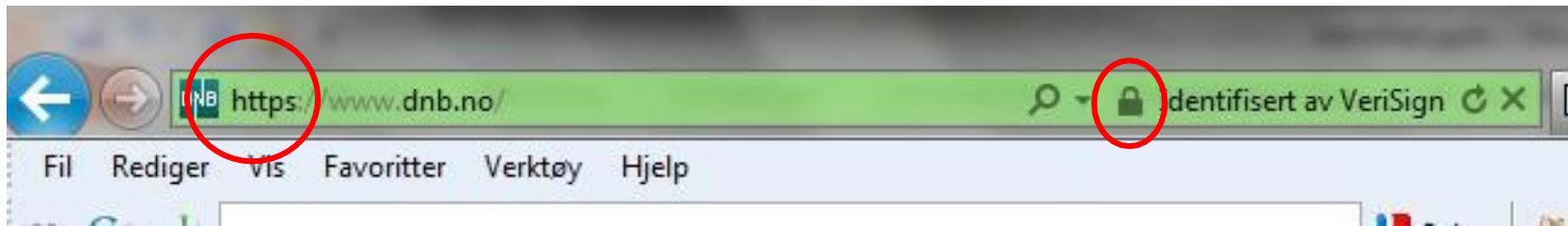
- Internet Explorer<sup>1</sup>
  - Edge<sup>1</sup>
  - Firefox<sup>1+2</sup>
  - Chrome<sup>1+2</sup>
  - Safari<sup>2</sup>
  - Det er mange flere ...
- 
- Nettleser bør være oppdatert
  - Vær kritisk til hvor du surfer; usikre sider gir større fare for å bli infisert
  - Vær skeptisk til nettsteder som ikke bruker HttPs:// (sikre sider)
  - Usikre sider
    - 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.

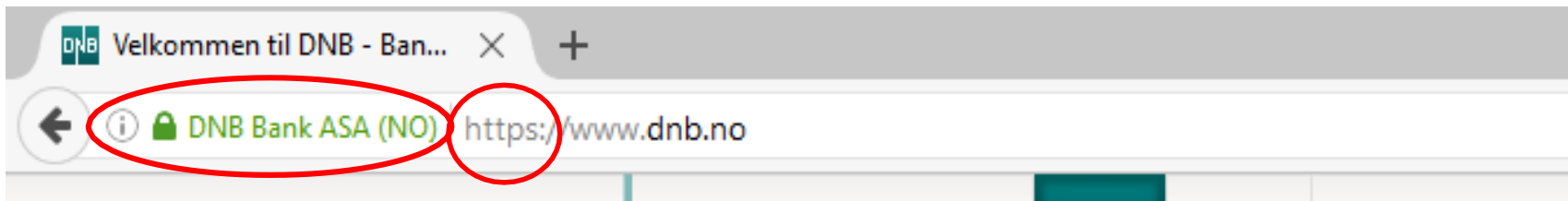
Slik vises det i Internet Explorer : hele adresselinje er grønn, https:// vises i adressen og du finner hengelåsen



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. Hengelsps endrer ikke farge med når du klikker på den kommer meldingen om VeriSign frem. Også her vises https:// i adressen

## 2-Trinns bekreftelse

et ekstra sikkerhetsnivå for innlogging av konto.

- En autentisering for innlogging
- Du logger du inn med noe du vet og noe du får
- Den gjør kontoen din sikrere fordi det hindrer andre å logge inn på din konto, selv om uvedkommende kjenner til ditt passord
- Men det å måtte taste inn en ekstra engangskode kan oppleves som tungvint for mange. Brukervennlighet og sikkerhet er som kjent motsetninger, hvor det ene nesten alltid vil gå utover det andre.
- «Oppskrifter hvordan man kan ta i bruk 2 trinns bekreftelse finner en på <https://nettvett.no/2-trinns-bekreftelse/>

# 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**
- **Prisene er veldig reduserte**
- **Dårlig språk**
- **Rare nettadresser** Eksempler: [www.billigburbery.com](http://www.billigburbery.com), [www.billignikefreerunsko-norge.com](http://www.billignikefreerunsko-norge.com), [www.cheapfreeonsale.org](http://www.cheapfreeonsale.org).
- **Nettadresser og butikknavn som ikke stemmer overens** Eksempel: en butikk har nettadressen [www.jakkesalg.eu](http://www.jakkesalg.eu) mens det inne på nettsiden står at den heter Canada Goose Norge.
- **Dårlig kvalitet** Forbrukerombudets liste over falske nettbutikker: [www.forbrukerombudet.no/netthandel/falske-nettbutikker](http://www.forbrukerombudet.no/netthandel/falske-nettbutikker)
- **Bruk Google**

# 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 f.eks. ved opprettelse av mobilabonnement)
- **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)
- **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)

## Andre betalingsmuligheter:

- Debetkort
  - Kontooverføring
  - Faktura
  - PayPal
  - Sjekk???
- (brukes fortsatt i en god del land. Gebyr for å løse inn en sjekk er ca. kr.300,- )

# HELST IKKE BRUK ET ÅPENT TRÅDLØS NETTVERK

- **Ikke bruk usikre nettverk:** hold deg til sikre nettverk eller mobildata. Nå tilbyr alle mobilselskaper 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.
- **Skru 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).

# Skylagring

- OneDrive
- Dropbox
- iCloud
- Box
- Google Foto
- Osv. osv.

Disse skylagringstjenester kjennetegnes av:

- ekstern lagring
- en del av disse har automatisk synkronisering, dvs. at f.eks. bildene blir lagret automatisk i skyen

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 sikkerhetskopi ofte nok?



# 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 tomte 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 )

# Installer tilleggsprogrammer for ekstra sikkerhet som Antimalware og Antispyware

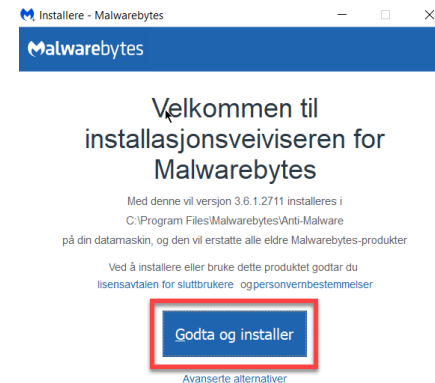
## 1. Anti-Malware program

- Antimalware program kan du laste ned gratis fra Malwarebyte <https://www.malwarebytes.com/mwb-download/>

- Velg Download free



- Følg så anvisninger for å laste ned programmet.



- Du vil nå i første omgang installere en 14 dagers prøversjjon av Pro-versjonen. Etter de 14 dager vil du få et spørsmål om du vil fortsette med Pro-versjonen (betal versjonen). Da velger du nei takk, og kan så fortsette med den gratis versjonen fremover.
- Etter at programmet har startet trykker du på Skann nå. Den skanningen kan ta litt tid. Dersom det etter skanningen er funnet feil, velg «Karantene». Feilene blir fjernet.

## 2. Anti-Spyware program

- Antispyware program kan du laste ned gratis fra

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

- Når du kommer til nettsiden, klikk på

A yellow rectangular button with the text "Download Free Edition" in black.

- Følg deretter anvisninger på skjermen, dvs. vanlig framgangsmåte for nedlasting

OBS!! På slutten kommer dette bilde.

**Ikke trykk "Enter" men trykk på «Decline»**

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

SUPERAntiSpyware Professional Trial



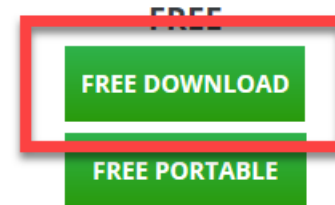
# Installer program for sikker avinstallering og for rensing av harddisk

## 1. Sikker avinstallering

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](http://www.revouninstaller.com/revo_uninstaller_free_download.html)
- Litt nede på siden til Revo Uninstaller finner du Free Download. Trykk på den.

Revo  ninstaller



- Følg så anvisninger på skjermen, dvs vanlig framgangsmåte for nedlasting av programmer.

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

Revo Uninstaller 2.0.1

Avinstallerer Verktøy Jaktmodus Alternativ Avinstallerer Oppdatere programlisten Vis Hjelp Upgrade to Pro-50%OFF

Søk etter:  
Navn

Program	Størrelse	Versjon	Type	Installering...	Firma	Webside	Kommentar
Adobe Acrobat Reader DC - Norsk	411,48 MB	15.020.20039	32-bit	14.10.2016	Adobe Systems Corpora...	http://www.adobe.com/...	
Adobe Creative Cloud	239,97 MB	3.8.0.310	32-bit	28.09.2016	Adobe Systems Corpora...		
Adobe Flash Player 23 NPAPI	5,90 MB	23.0.0.185	32-bit	14.10.2016	Adobe Systems Corpora...	http://www.adobe.com/...	
Adobe Photoshop CC 2015.5	1,21 GB	17.0.1	32-bit	30.09.2016	Adobe Systems Corpora...	http://www.adobe.com/...	
Adobe Photoshop CS6	116,21 MB	13.0	32-bit	14.10.2016	Adobe Systems Corpora...		
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	4.1.6	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.

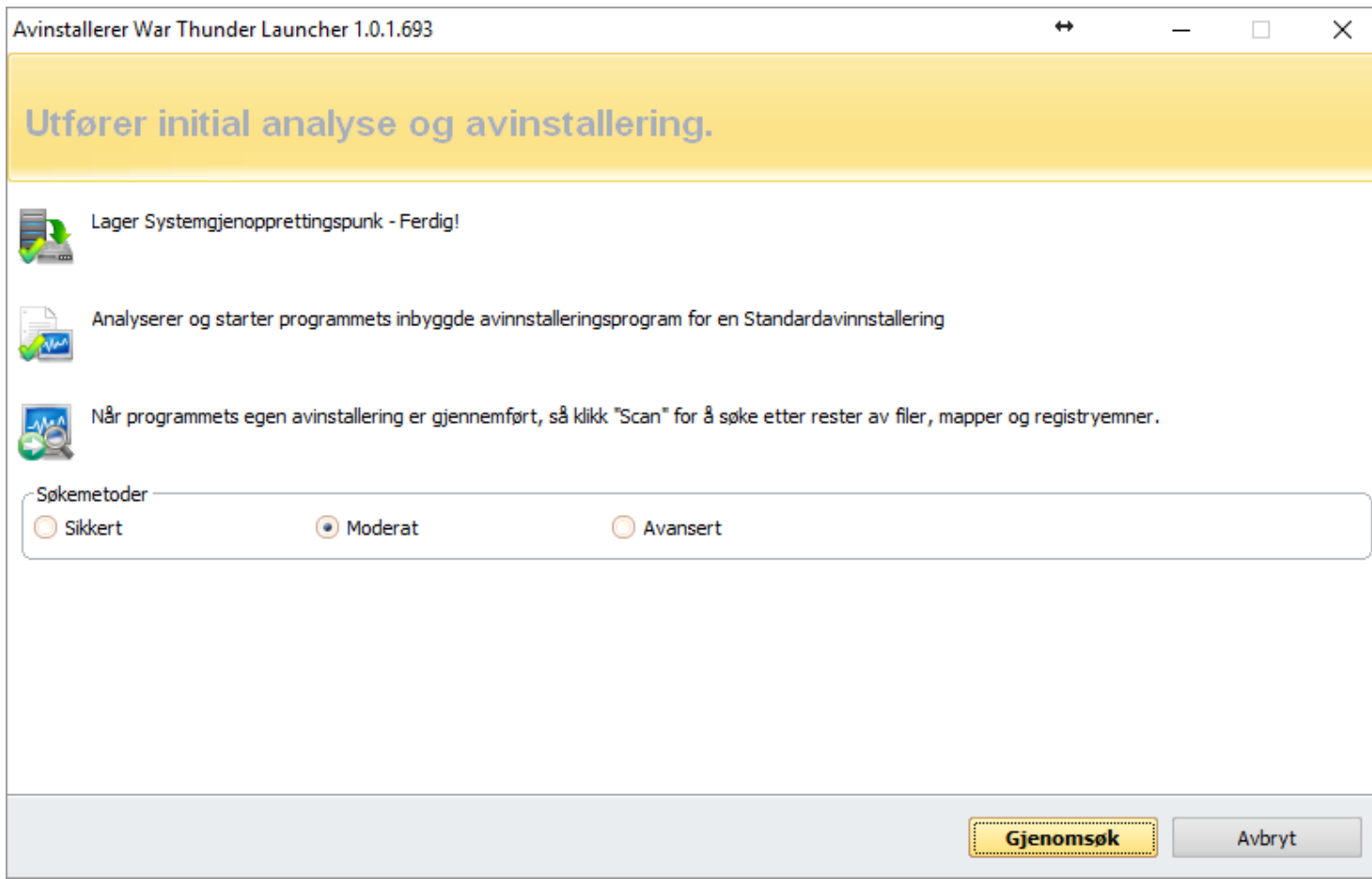
Installerte: 105

lysilde 16 av 17 Norsk (bokmål)

Activate Revo Uninstaller Pro Like us

Notater Kommentarer 71%

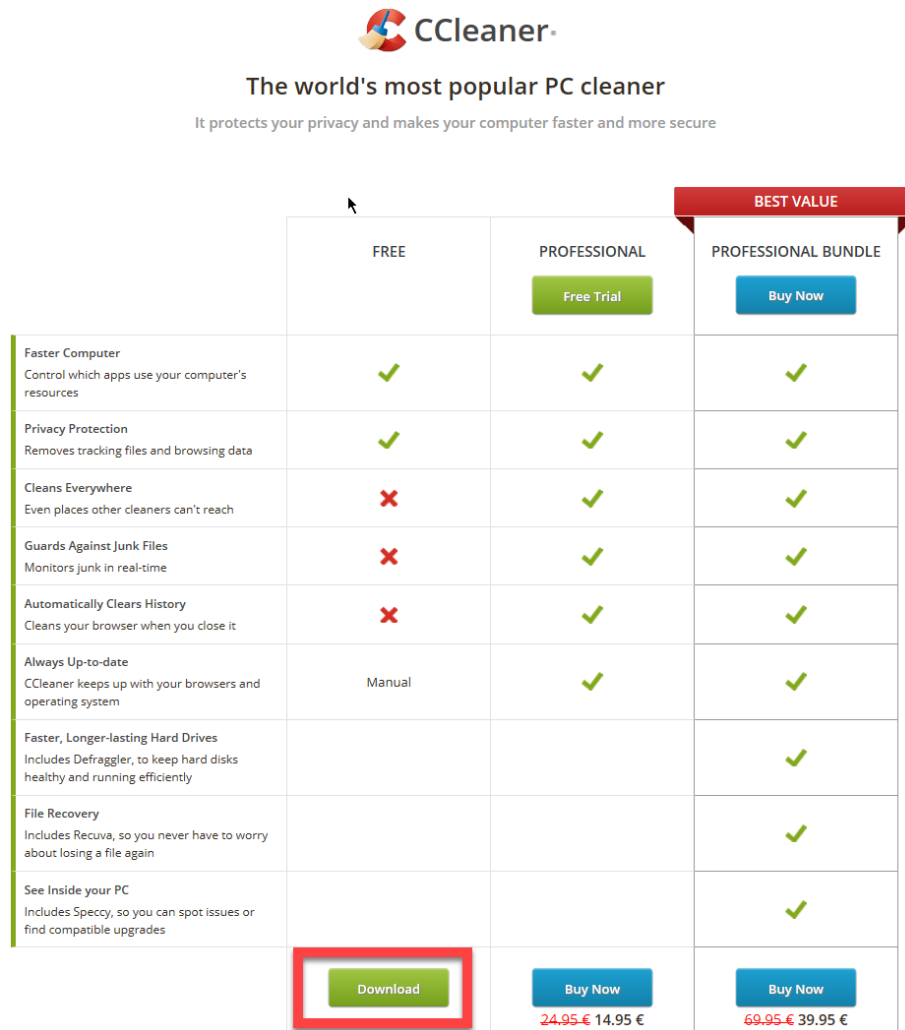
- Programmet avinstalleres nå.
- Etter dette må maskinen gjennomføres om det fortsatt ligger (skjulte) filer, som tilhører programmet du har avinstallert, igjen på din PC. La valget stå på Moderat og trykk Gjennomfør.
- Dersom det finnes fortsatt filer på din PC som tilhører programmet, vil disse komme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



## 2. Rensing av harddisk

Et gratis program for rensing av harddisk er CCleaner.

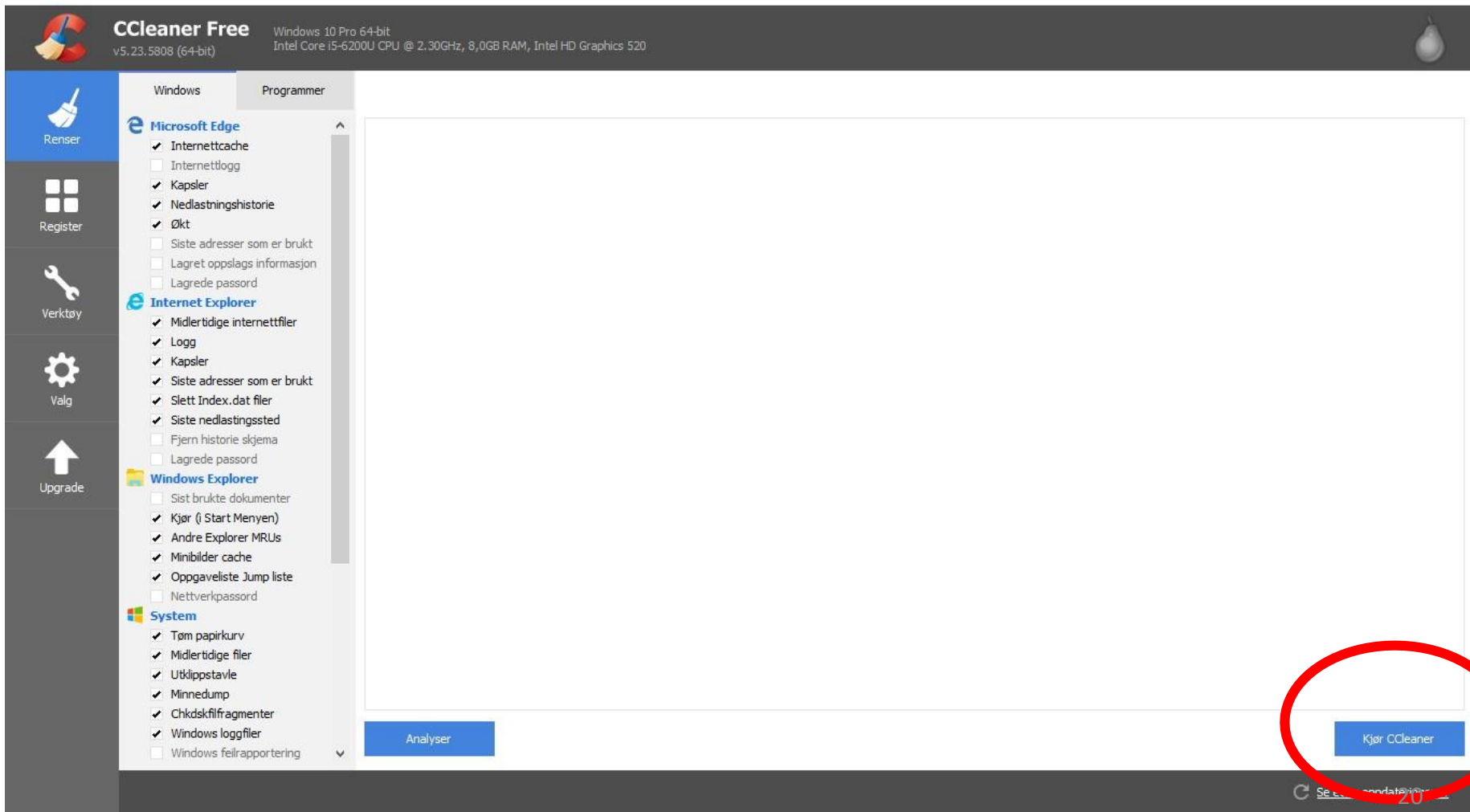
- Last ned CCleaner fra <https://www.piriform.com/ccleaner/download>
- Dette vises. Velg nedenfor "Free" knappen "Download"



The screenshot shows the CCleaner website's pricing page. At the top, the CCleaner logo is displayed next to the text "The world's most popular PC cleaner" and "It protects your privacy and makes your computer faster and more secure". Below this, there are three pricing columns: FREE, PROFESSIONAL, and PROFESSIONAL BUNDLE. The PROFESSIONAL BUNDLE column is marked as "BEST VALUE". Each column has a "Free Trial" or "Buy Now" button. The FREE column has a "Download" button highlighted with a red box. The table below compares features across the three options.

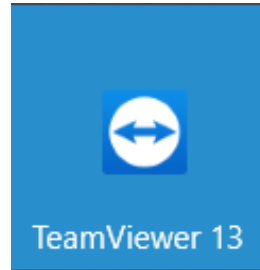
	FREE	PROFESSIONAL	PROFESSIONAL BUNDLE
		Free Trial	Buy Now
Faster Computer Control which apps use your computer's resources	✓	✓	✓
Privacy Protection Removes tracking files and browsing data	✓	✓	✓
Cleans Everywhere Even places other cleaners can't reach	✗	✓	✓
Guards Against Junk Files Monitors junk in real-time	✗	✓	✓
Automatically Clears History Cleans your browser when you close it	✗	✓	✓
Always Up-to-date CCleaner keeps up with your browsers and operating system	Manual	✓	✓
Faster, Longer-lasting Hard Drives Includes Defraggler, to keep hard disks healthy and running efficiently			✓
File Recovery Includes Recuva, so you never have to worry about losing a file again			✓
See Inside your PC Includes Speccy, so you can spot issues or find compatible upgrades			✓
	Download	Buy Now 24.95 € 14.95 €	Buy Now 69.95 € 39.95 €

- 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.





## ..... og til slutt et Fjernstyringsprogram .....



Dersom du trenger hjelp fra Seniorsnett, for et problem du opplever på din PC, kan det være veldig nyttig at du har et fjernstyringsprogram installert på din PC.

Et fjernstyringsprogram gjør at den du får hjelp av til å løse problemet på din PC, vil kunne få tilgang til din PC og kunne styre den mens problemet løses. Dette er en såkalt engangs-tilgang, dvs. dersom tilgangen brytes må du først gi tillatelse for evt. ny tilgang til din PC. Det er du som styrer dette.

Fjernstyrings programmet som Seniorsnett bruker heter Teamviewer.

Hvordan du laster det ned finner du ved å trykke på lenken nedenfor

<https://www.seniornett.no/wp-content/uploads/2018/01/Teamviewer-1.pdf>