



Larvik
kommune

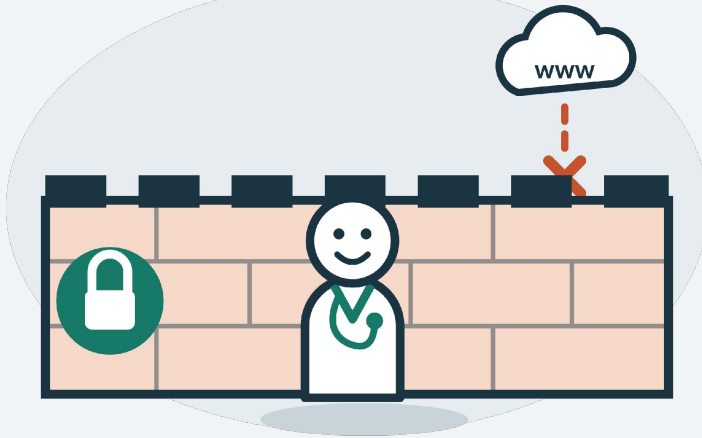
Herdet nettleser og proxy

Lisenskostnad: **0** kr



Nils Tore Lia

Fra «sikker sone» til ...?



Før: sikker sone

Sikkerheten lå i murene



Nå: åpen nettleser?

Sikkerheten hviler på brukeren

**Målet er ikke å gjøre helsearbeidere
til sikkerhetseksperter.
Målet er at de ikke trenger å bli det.**



Jo smartere nettleseren blir, jo mer deler den

Nyttig i hverdagen, men mer data forlater nettleseren enn de fleste er klar over.



AI-assistent

Kan lese siden du har åpen – også pasientjournalen – og sende innholdet til Copilot eller Gemini



Søkeforslag og telemetri

Det du skriver i adressefeltet, kan nå søkemotoren før du trykker Enter – også det du angir på. Krasjrapporter kan ta med innhold fra siden



Skystavekontroll

Alt du skriver i tekstfelt, også journalnotater, kan sendes til skyen for retting



Synkronisering med sky-konto

Historikk, åpne faner, favoritter, **skjemadata** og passord lagres i skyen og deles med andre enheter



Oversettelse av tekst

Sideinnholdet sendes til skyen når siden oversettes



Høytlesing og bildesøk

Tekst som leses høyt og bilder du søker på, kan sendes til skyen

Brukere flytter data ut av nettleseren

... ofte uten å vite det.

Data kopieres ut lokalt

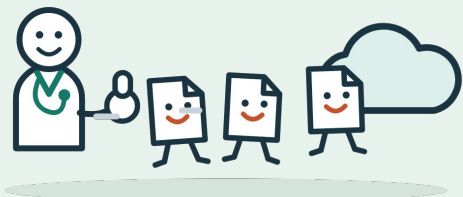


- Pasientdata kan kopieres fritt til usikre apper og nettsider (Ctrl-C, Ctrl-V)
- Nedlastede dokumenter kan bli liggende i standardmappe på klienten lenge

Data synkroniseres til sky



- OneDrive/Google Drive synkroniserer filer og mapper til sky
- «Cloud Clipboard» gjør det kopierte innholdet tilgjengelig på andre enheter



Systemet stoppet meg ikke – så da var det vel lov?

Andre utfordringer

SSO, tredjepartskode og sporbarhet



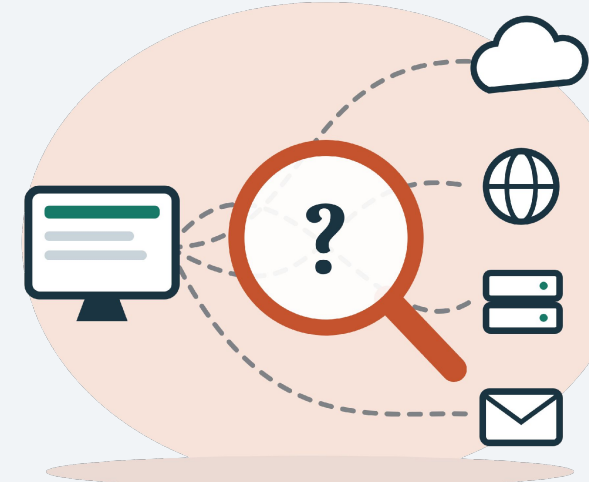
Single sign-on

Ulåst PC = åpen journal



Nettleserutvidelser

Leser alt, og kan endres uten varsel



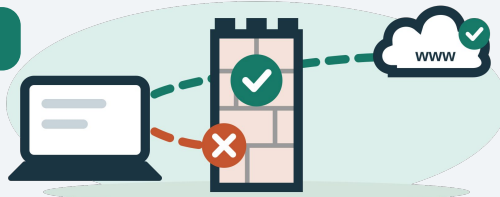
Manglende sporbarhet

Mange nettveier, ingen samlet logg

Fortsatt trygt – uten mastergrad i sikkerhet

Tre lag som automatisk hjelper de ansatte å unngå lekkasjer

Lag 1



Nettverkssikkerhet

- Proxy med «deny-by-default» – kun hvitlistede domener slipper gjennom
- I tillegg begrenser brannmuren hvilke adresser proxyen får nå

Lag 2



Nettleserherding

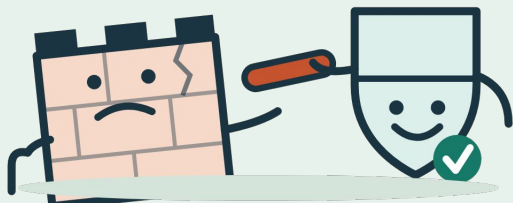
- Egen midlertidig Edge-profil, kryptert lokalt
- AI, stavekontroll, synk, søkeforslag og oversettelse er slått av
- Nedlastinger havner i egen mappe som ryddes automatisk
- Kopiering og utklipp blokkeres

Lag 3



Identitet og tilgang

- Brukeren bekrefter egen identitet ved oppstart
- Fagsystemene kan kun nås via sikret nettleser
- All trafikk går gjennom én logget vei (brannmur-, proxy- og klientlogg)



Sikker sone er dø(d)ende. Møt arvtageren: Sikret nettleser...

LIVE DEMO



En forenklet versjon av skriptet

Lavthengende frukt

- Kan tas i bruk uten endringer i nettverk eller AD/Entra ID
- Gir isolert profil, herdet Edge og automatisk opprydding



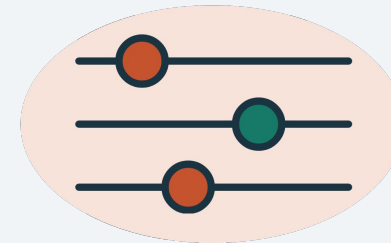
Konfigurasjon

Alt som kan endres, samlet øverst i fila

```
@echo off
setlocal
cls

REM --- Konfigurasjon ---
set "BrowserExe=msedge.exe"
set "LaunchTarget=https://www.larvik.kommune.no/"
set "BaseDir=%temp%\SecureBrowser"
set "ProfileName=DEMO"
set "ProfileDir=%BaseDir%\%ProfileName%"
set "DownloadDir=%BaseDir%\Download"
set "MarkerFile=%ProfileDir%\ProfileAgeMarker.txt"
set "PrefFile=%ProfileDir%\Preferences"
set "JsonDllDir=%DownloadDir:=\%\"

REM Tidsfrister for opprydding i dager
set "ProfileMaxAgeDays=-7"
set "DownloadMaxAgeDays=-2"
```



Hva skjer her?

- Profil, nedlastinger og innstillinger ligger under %temp%
- Profilnavnet DEMO gir en egen, navngitt profilmappe
- Negative tall er forfiles-syntaks: eldre enn 7 og 2 dager

Grunnmappe og kryptering

Mappa opprettes én gang og krypteres på disk

```
REM --- Grunnmappe og kryptering ---  
if not exist "%BaseDir%" mkdir "%BaseDir%"  
cipher /e "%BaseDir%" >nul
```



Hva skjer her?

- Oppretter nedlastingsmappe (hvs den ikke finne)
- cipher /e slår på EFS-kryptering for mappa (alt som senere opprettes under den arves)
- Nedlastede filer ligger dermed kryptert lokalt

Opprydding: profilens levetid

Markørfila bestemmer når profilen kastes

```
REM --- Opprydding av filer ---  
REM Sletter profilmarkøren hvis den er 7 dager gammel,  
REM og fjerner profilen når markøren mangler
```

```
if exist "%MarkerFile%" forfiles /P "%ProfileDir%" ^  
    /M ProfileAgeMarker.txt /D %ProfileMaxAgeDays% ^  
    /C "cmd.exe /c del /q @path" >nul 2>&1
```

```
if not exist "%MarkerFile%" rmdir /s /q "%ProfileDir%"
```



Hva skjer her?

- forfiles /D -7 treffer bare filer eldre enn sju dager
- Er markøren gammel, slettes den
- Neste linje ser at markøren mangler, og fjerner hele profilen
- Slik nullstilles profilen automatisk hver uke

Opprydding: midlertidige filer

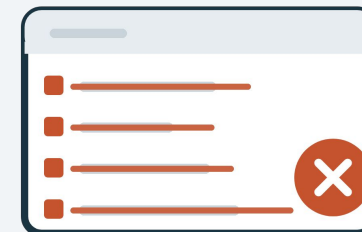
Historikk, cache og gamle nedlastinger fjernes

```
REM Tømmer midlertidig nettleserdata fra profilen
if exist "%ProfileDir%" (
    for %%X in (History History-journal ^
        "Visited Links" "Top Sites") do ^
        del /q /f "%ProfileDir%\%%~X" >nul 2>&1

    for %%Y in (Cache "Code Cache" GPUCache ^
        Sessions "Service Worker" CacheStorage) do ^
        rmdir /s /q "%ProfileDir%\%%~Y" >nul 2>&1
)

REM Rydder nedlastinger eldre enn 2 dager
if exist "%DownloadDir%" forfiles /P "%DownloadDir%" ^
    /M * /D %DownloadMaxAgeDays% ^
    /C "cmd.exe /c del /q @path" >nul 2>&1

REM --- Oppretting av undermapper ---
if not exist "%ProfileDir%" mkdir "%ProfileDir%"
if not exist "%DownloadDir%" mkdir "%DownloadDir%"
```



Hva skjer her?

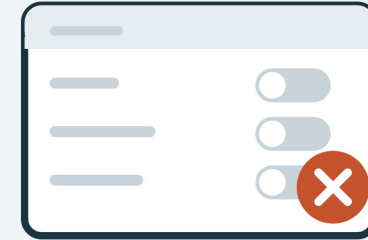
- Første løkke sletter filer: historikk, besøkte lenker, toppsider
- Andre løkke fjerner hele cache- og sesjonsmapper
- Økten starter dermed uten spor fra forrige gang
- Til slutt gjenopprettes mappene som mangler

Preferences: personvern og støy

Fila skrives på nytt ved hver oppstart

REM Én lang linje i skriptet – her brutt opp for lesbarhet

```
> "%PrefFile%" echo {"pref_version":1,  
  "edge_shopping_assistant_enabled":false,  
  "edge_tab_services_enabled":false,  
  "alternate_error_pages":{"enabled":false},  
  "resolve_navigation_errors_use_web_service":  
    {"enabled":false},  
  "localsuggest":{"enabled":false},  
  "trendingsuggestions":{"enabled":false},  
  "omnibox":{"scope_search_enabled":false},  
  "ntp":{"enable_prerender":false},  
  "payments":{"can_make_payment_enabled":false},  
  "edge_wallet":{"wallet_checkout_enabled":false},  
  "credentials_enable_service":false,  
  "enable_do_not_track":true,  
  "autofill":{"credit_card_enabled":false,  
    "profile_enabled":false},  
  "devtools":{"f12_shortcut":{"enabled":false}},
```



Hva skjer her?

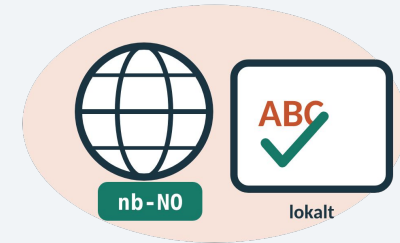
- Slår av tjenester vi ikke trenger
- Sender ikke URL-er til leverandør når en side ikke lastes
- Passord skal ikke lagres i profilen
- Kortopplysninger og adresser lagres ikke og fylles ikke ut automatisk

Preferences: språk, staving og tema

Norsk språk, lokal stavekontroll og egen nedlastingsmappe

```
"profile":{"name":"%ProfileName%",
  "password_manager_enabled":false},
"translate":{"enabled":false},
"intl":{"accept_languages":"nb-NO,nb,no,en-US,en",
  "selected_languages":"nb-NO,nb,no"},
"spellcheck":{"use_spelling_service":false,
  "dictionaries":["nb-NO","nb"]},
"download":{"default_directory":"%JsonDllDir%",
  "prompt_for_download":false},
"browser":{"show_hub_sidebar":false,
  "show_copilot_icon":false,
  "accent_color_value":-6404281,
  "enable_spellchecking":true},
"edge":{"compose_inline_enabled":false,
  "sidebar_state":{"is_copilot_pinned":false}},
"autogenerated":{"theme":{"color":-6404281}}}

if not exist "%MarkerFile%" >"%MarkerFile%" ^
  echo Profil opprettet: %date% %time%
```



Hva skjer her?

- Oversettelse og skybasert stavekontroll er av; stavekontroll skjer lokalt med norsk ordliste
- Nedlastinger går rett til egen mappe, uten spørsmål
- Copilot og KI-skriveassistent er skjult og slått av
- Eget tema gjør vinduet gjenkjennelig

Oppstart av nettleseren

Isolert profil, fullskjerm og norsk språk

```
REM --- Oppstart av nettleser ---
title Sikret Nettleser - DEMO

REM Én linje i skriptet – her brutt opp for lesbarhet
START "" "%BrowserExe%" ^
    --start-maximized ^
    --disable-extensions ^
    --lang=nb-NO ^
    --accept-lang=nb-NO,nb,no,en-US,en ^
    --user-data-dir="%BaseDir%" ^
    --profile-directory="%ProfileName%" ^
    --no-proxy-server ^
    --no-first-run ^
    --no-default-browser-check ^
    --disable-sync ^
    ... "%LaunchTarget%"
```



Hva skjer her?

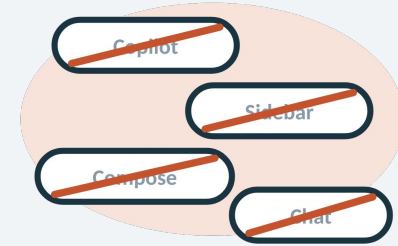
- Egen user-data-dir: ingen kobling til brukerens vanlige Edge
- --disable-extensions blokkerer alle utvidelser
- I denne demoen går trafikken utenom proxy
- Synkronisering til sky er slått av

Oppstart: funksjoner som slås av

Resten av flaggene i START-linja

```
--disable-domain-reliability ^
--no-experiments ^
--disable-background-networking ^
--disable-gpu ^
--disable-features=msEdgeSidebarV2, ^
msUndersideButton,msEdgeChat,msEdgeCopilot, ^
HttpsUpgrades,msTabOrganization, ^
TabOrganization,msEdgeVideoTranslate, ^
msCompose,msEdgeCompose,SpellingService, ^
msShowSignInIndicator ^
--site-per-process ^
--no-pings ^
--disable-background-mode ^
"%LaunchTarget%"

exit /b 0
```



Hva skjer her?

- Copilot, chat, sidefelt og Compose startes ikke
- SpellingService hindrer skybasert stavekontroll
- Bakgrunnstrafikk, telemetriforsøk og pings er slått av
- --site-per-process gir full prosessisolering mellom nettsteder

Prøv selv: Sikret nettleser Light

Den forenklede versjonen, klar til å lastes ned

Tre ting før du starter

- Fila heter SikretNettleser-Light_v1.0.cmd.txt. Fjern .txt til slutt (lagt til for at fila ikke skal bli stoppet ved nedlasting).
- Ikke kopier koden fra lysbildene: den er brutt opp for lesbarhet. JSON- og START-linja må være én linje.
- Skriptet er et utgangspunkt. Test i eget miljø, og legg gjerne til proxy med hviteliste (Lag 1).



Skann for å laste ned

Eller klikk her: drive.google.com