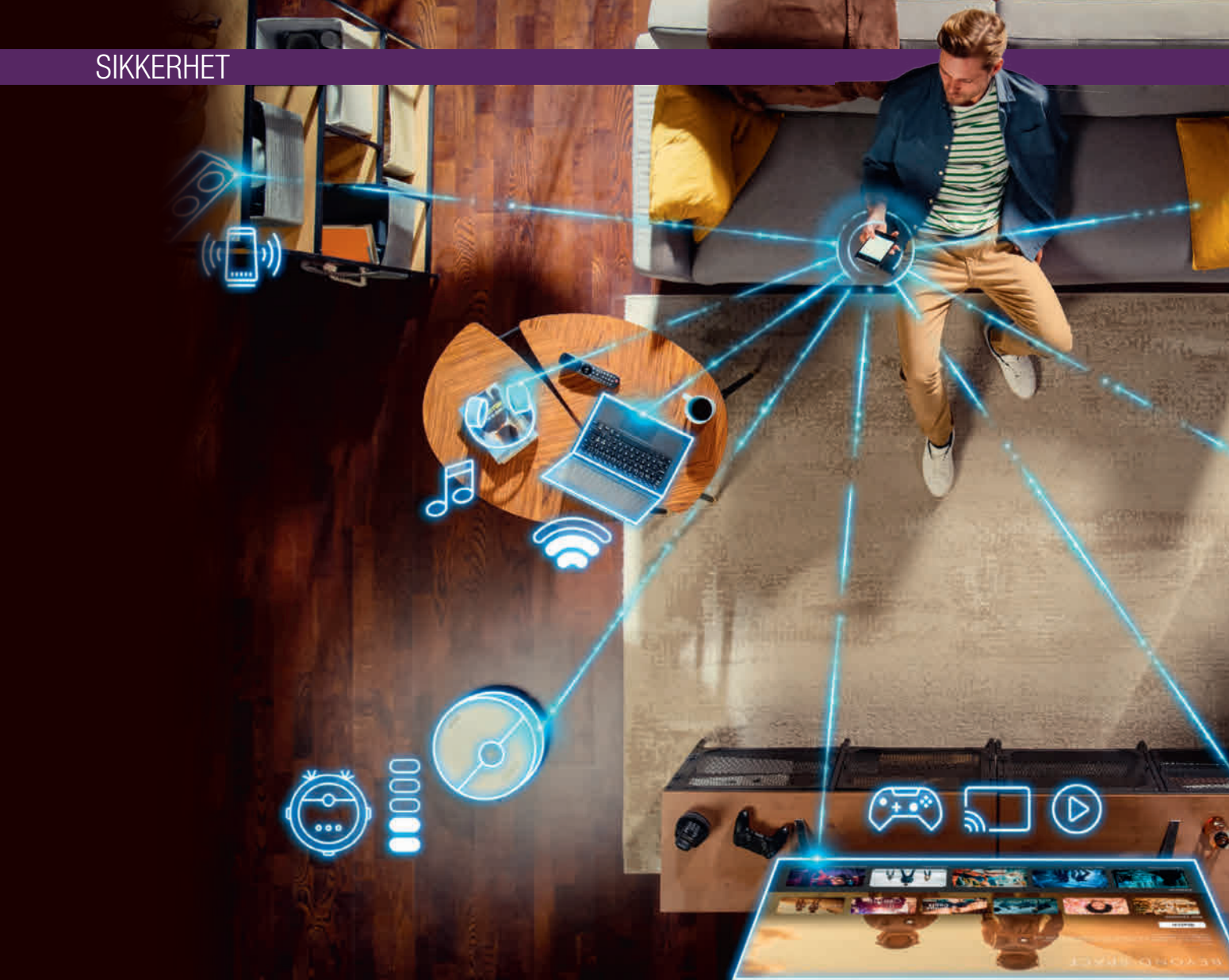




FOREBYGGING AV ANGREP MOT HJEMMENETTVERKET:

Hvordan sikre alle digitale enheter

Det holder ikke å bare sikre mobil og pc mot angrep fra nettet. Alle enheter som er på nett, kan være utsatt. Derfor bør du gi alt tilkoblet utstyr en grundig gjennomgang – jo før, jo heller.



Full sikkerhetssjekk

Har du utstyr som kan være utsatt for angrep fra nettet? Her ser du eksempler på enheter du bør sikre:

- Sonos eller andre smarthøytalere
- Nettverbskameraer
- Nettverbskriver
- TV-bokser som Google TV og Apple TV
- App-styrte stikkontakter
- Smart belysning
- Nettverbsdisker (NAS)
- Smart TV-apparater
- Trådløse ruter
- Gateway for styring av gardiner, lys og varme
- Spillkonsoller
- Smart dørklokke
- Robotstøvsuger
- App-styrt døråpner
- Hvitevarer med integrert Wi-Fi
- Værstasjon med nettverkstilgang



Journalist
Henning Rasmussen

Det er unektelig lite bærekraftig å skrote elektronikk som fortsatt virker og som du kanskje bruker til daglig. Det kan likevel være nødvendig hvis utstyret er koblet til internett og ikke lenger mottar sikkerhetsoppdateringer fra produsenten.

Farlige sikkerhetshull

Både sikkerhetseksperter og produsenter, men også kriminelle, oppdager nemlig fortløpende nye metoder for å skaffe seg uautorisert tilgang til enheter på hjemmenettverket.

Sårbarhetene blir gjerne rettet ved at produsenten sender ut en fastvareoppdatering til smarte stikkontakter, nettverbsdisker, overvåningskamera-

er og så videre. Dessverre er det de færreste produsenter som fortsetter å oppdatere slike enheter når de er mer enn fem år gamle.

Måtte vrake kameraer

Det fikk jeg selv smertelig erfare. I årvis hadde jeg tre grisedyre nettverbskameraer fra produsenten D-Link installert i heimen, og de fungerte upåklagelig selv om de var mer enn ti år gamle. På administrasjonssiden for kameraene oppdaget jeg imidlertid at den ferskeste oppdateringen fra produsenten var syv år gammel.

Hackere hadde med andre ord hatt syv år på seg til å finne et sikkerhetshull i de mange tusen kameraene av samme type som fantes over hele kloden. Derfor valgte jeg med tungt hjerte å levere dem til gjenvinning, selv om de sikkert kunne fungert i mange

år til. Kanskje har også du utstyr av eldre dato stående?

Det er flere ting du kan gjøre selv for å sikre gammelt utstyr. Du bør først og fremst sjekke at tilgangen til enhetene er beskyttet av et solid passord som du selv, og ikke produsenten, har valgt. I tillegg kan du passe på at det ikke er unødvendige åpne porter i ruter og at alle enheter er oppdatert med den nyeste fastvaren.

Er du usikker på hvilke enheter som er på nett, kan du begynne med å skanne hele nettverket ved hjelp av programmet Advanced IP Scanner. Det avslører alle tilkoblede enheter, og her kan du også se de respektive IP-adressene, som du må kjenne for å få tilgang til enheten i nettleseren. Deretter er du klar til å følge våre enkle veiledninger for å sikre alt du har av ting som er på nett.



Advanced IP Scanner

Programmet skanner hele nettverket og viser alle tilkoblede enheter.

Språk
Engelsk

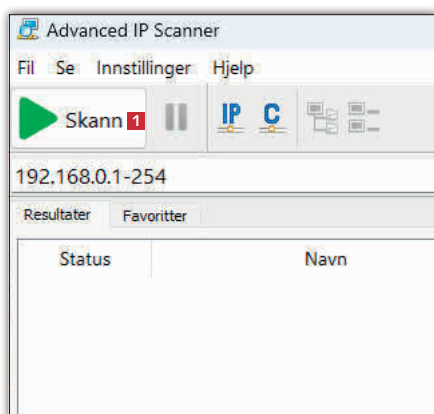
Virker med
Windows 10 og 11

Programmet laster du ned fra:
komputer.no/2511

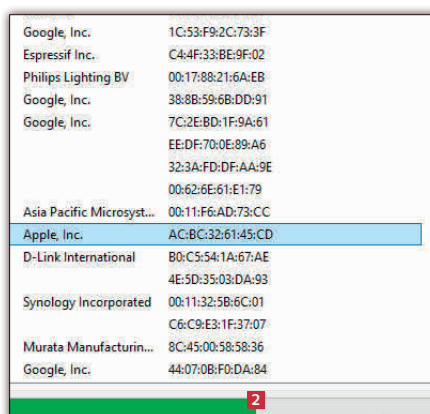


Først må du finne alle tilkoblede enheter

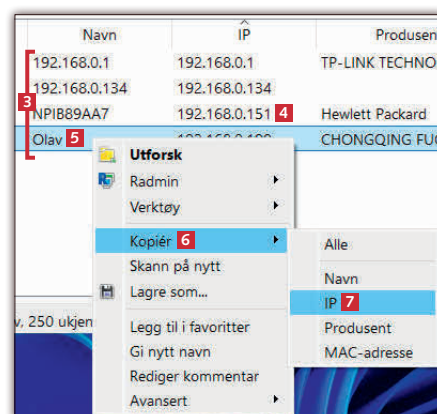
Du må kjenne IP-adressene til alle enheter, slik at du kan logge inn og sjekke sikkerheten. Adressene finner du lett med Advanced IP Scanner.



1 Last ned og installer Advanced IP Scanner fra nettsiden vår. Når du starter programmet, klikker du på **Skann 1** øverst til venstre.



2 Vent til hele nettverket er gjenomgått, altså når den grønne forløpsindikatoren har fylt ut linjen nederst i vinduet **2**.

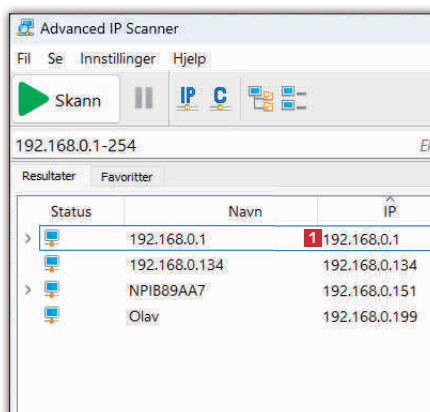


3 Nå vises enhetene **3** og deres respektive IP-adresser **4**. Høyreklikk på en enhet **5**, velg **Kopier 6** og **IP 7**. Sett inn adressen i nettleseren.

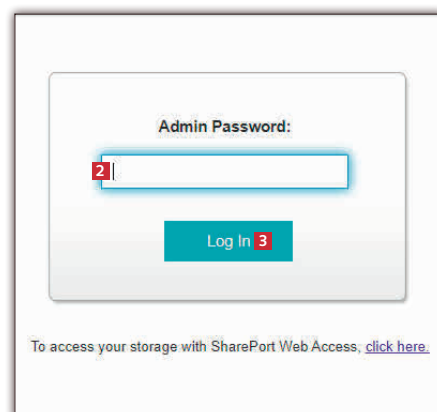


Oppdater ruter

Den trådløse ruter er koblet direkte til "verdensveven". Derfor er det viktig å alltid holde den oppdatert med den nyeste fastvaren.



1 Åpne Advanced IP Scanner-programmet, og skann pc-en. Øverst i listen over enheter finner du ruter og IP-adressen **1** til denne. Den trenger du i neste trinn.

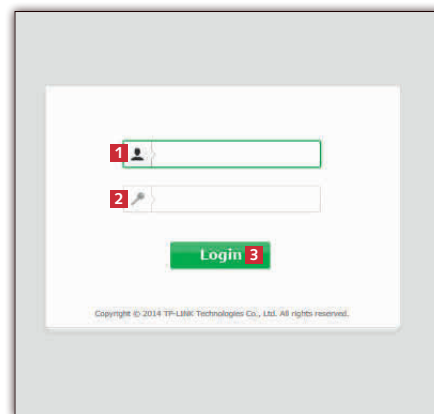


2 Åpne nettleseren og skriv adressen til ruter i adressefeltet. Trykk på **Enter**. Oppgi passordet til ruter **2**, som er valgt av deg eller produsenten. Klikk på **Log In 3**.

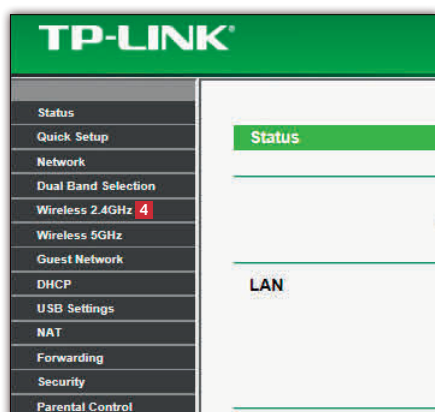


Velg den sterkeste krypteringen

Den trådløse tilkoblingen mellom de ulike enhetene og ruterens sikres ved hjelp av kryptering, og det finnes flere typer. Pass på at du velger den nyeste og sikreste standarden.



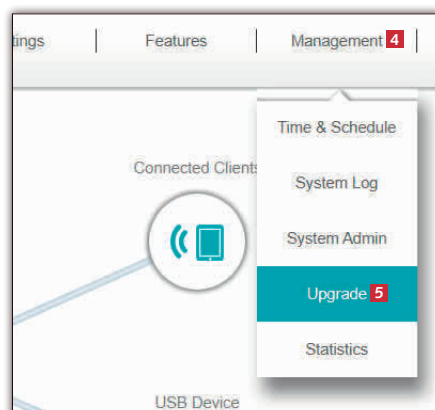
1 Åpne nettleseren og skriv ruter-adressen i adressefeltet. Trykk på **Enter**. Oppgi brukernavnet **1** og passordet **2** til ruterens (står i brukerveiledningen). Klikk på **Login 3**.



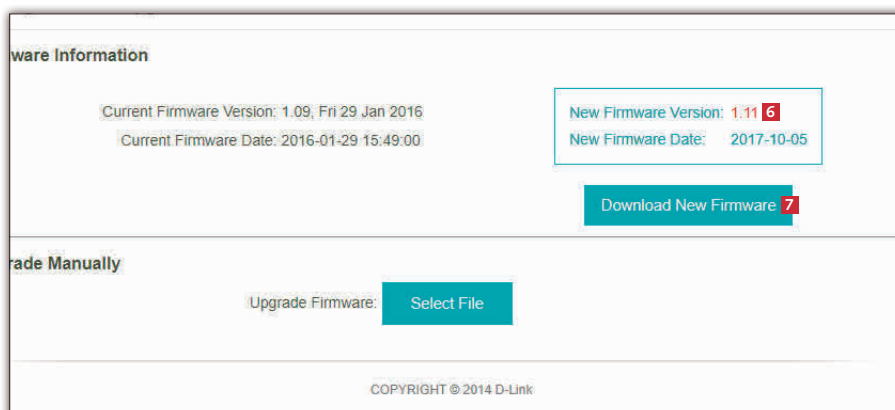
2 Klikk på **Wireless 2.4GHz 4** i menyen for å endre innstillinger for det trådløse 2,4 GHz-nettet.



3 Klikk på **Wireless Security 5**. Marker **WPA/WPA2 Personal 6** eller WPA3, hvis tilgjengelig. Velg **Automatic 7**, **AES 8** og skriv et passord som er vanskelig å gjette **9**. Klikk på **Save**. Ruterens starter på nytt, og så snart den er oppe og går, logger du igjen på nettverket fra alle enhetene. Gjenta prosessen for 5 GHz-nettet.



3 På denne rutermodellen skal man klikke på **Management 4** og velge **Upgrade 5**. På andre kan det være **Advanced** eller **Firmwareupgrade**.



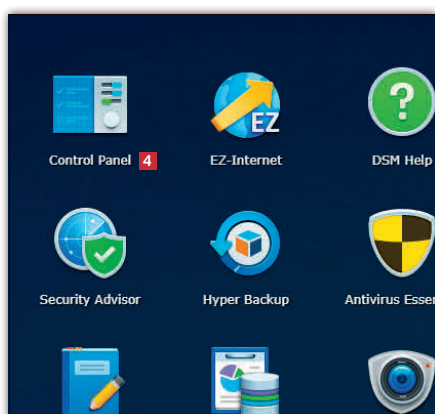
4 Her vil du kunne se om det finnes ny fastvare til ruterens **6**. I så fall klikker du på **Download New Firmware 7** for å laste ned og installere den. Til slutt dobbeltsjekker du at du faktisk har den nyeste fastvaren.



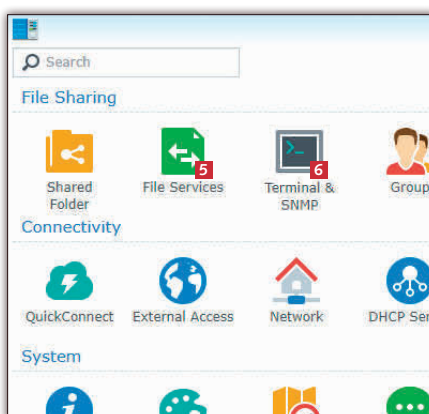


Lukk åpne porter på nettverksdisken

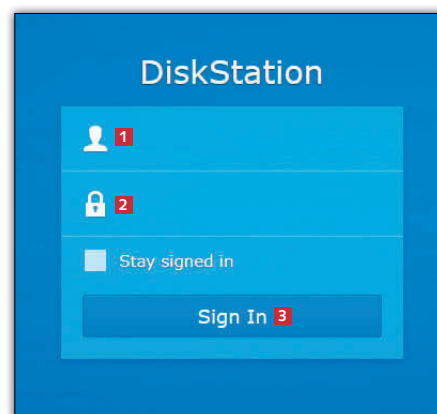
Dagens nettverksdisker (NAS) har mengder av funksjoner i tillegg til lagring av filer. Derfor må du sjekke om portene til tjenerfunksjonene er lukket, hvis du likevel ikke benytter deg av disse.



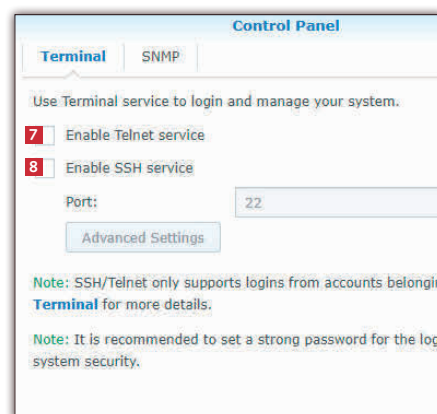
2 Finn **Kontrollpanelet** **4** for enheten. Det vil se forskjellig ut og ha ulike navn avhengig av merke og modell. Her har vi en nettverksdisk fra Synology.



3 Åpne NAS-porter finnes normalt under **File Services** **5** eller **Terminal & SNMP** **6**.



1 Finn adressen til NAS-enheten med Advanced IP Scanner. Åpne nettleseren og skriv adressen. Trykk på **Enter**. Oppgi brukernavn **1** og passord **2**. Klikk på **Sign in** **3**.

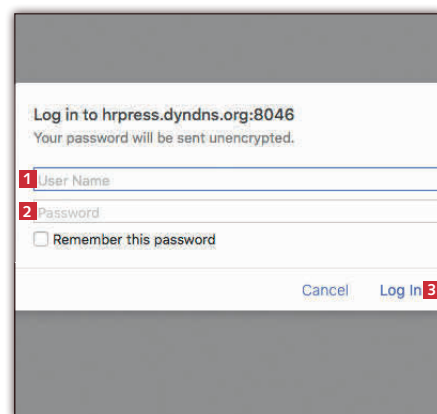


4 Pass på å fjerne hakene ved **Enable Telnet service** **7** og **Enable SSH service** **8**, hvis ikke dette er noe du bruker aktivt. Klikk på **Bruk**. Nå er risikoen eliminert.



Velg sterkere passord

Når du kjøper nytt utstyr, er det som regel sikret med et standardpassord fra produsenten. Det bør du snarest endre til et godt og robust passord du har valgt selv. Her viser vi hele prosessen for et IP-kamera.

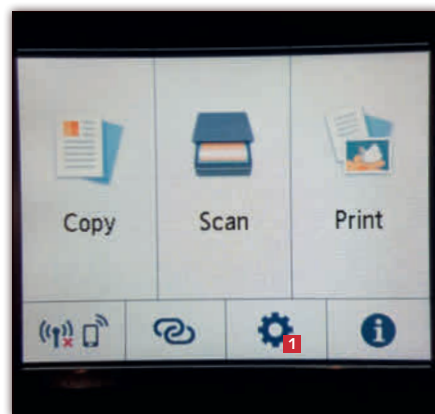


1 Finn adressen til nettverkskameraet i Advanced IP Scanner, og skriv den i adressefeltet til nettleseren. Trykk på **Enter**. Oppgi brukernavn **1** og passord **2**, og klikk på **OK** **3**.



Oppdater alt utstyret

Ikke alt utstyr holdes oppdatert fortløpende og automatisk av produsenten. Derfor bør du med jevne mellomrom sjekke om det finnes nye oppdateringer. Det gjelder også for enheter som skrivere, hvis de er koblet til nettverket.



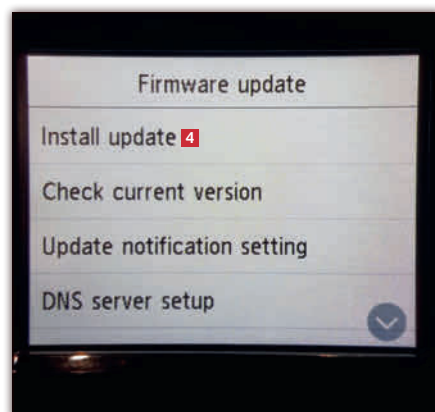
1 På en nyere Canon-skriver med trådløs tilgang til internett ser hovedmenyen på den lille skriver-skjermen ut som vist her. Her skal man trykke på tannhjulet **1**.



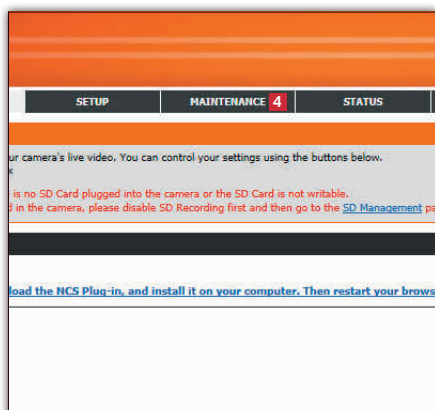
2 Velg **Device settings** **2**, "enhetsinnstillinger" eller lignende hvis menyen er på norsk.



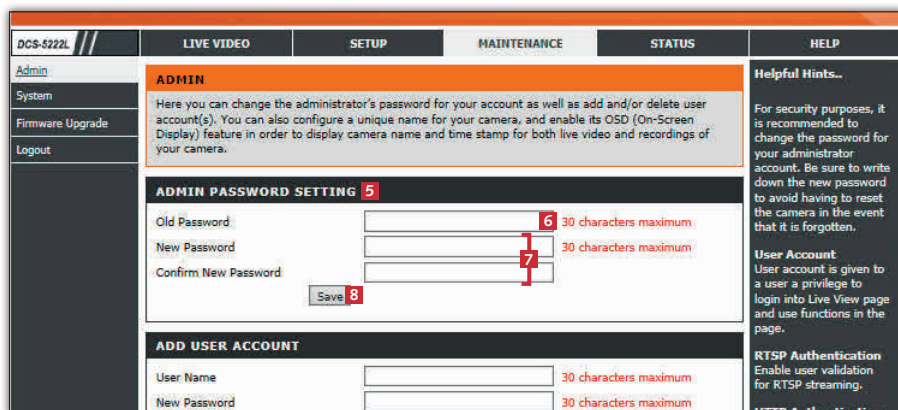
3 Bla helt ned i menyen og trykk på **Firmware update** **3**, eventuelt "fastvareoppdatering" eller lignende.



4 Trykk på **Install update** **4**, og følg veiviseren som oppdaterer skriveren med den nyeste fastvaren. Dermed har du redusert faren for angrep mot skriveren fra nettet.



2 Her er vi inne på siden til et IP-kamera fra D-Link. Sidene er forskjellige fra produsent til produsent. Når det gjelder D-Link, må man først klikke på **Maintenance** **4**.



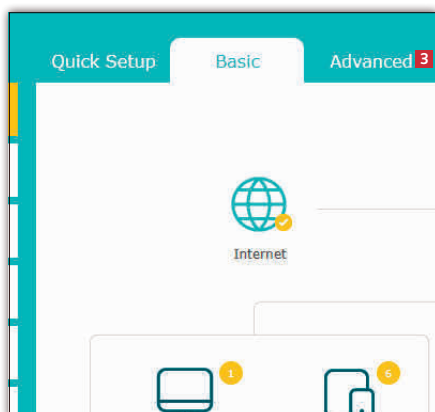
3 Under **Admin password setting** **5** oppgir du det gamle passordet til enheten **6**. Deretter skriver du det nye passordet to ganger **7**. Klikk på **Save** **8** for å lagre innstillingene. Dermed har du gjort det vanskeligere for uvedkommende å ta seg inn på enheten.



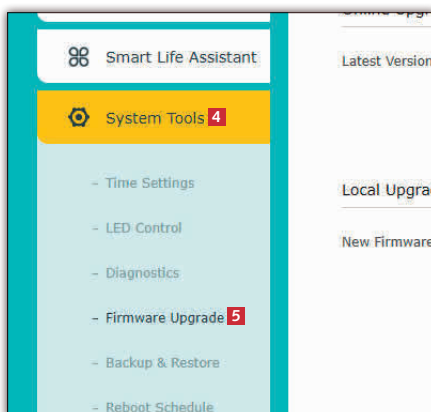


Oppdateres ikke lenger enhetene?

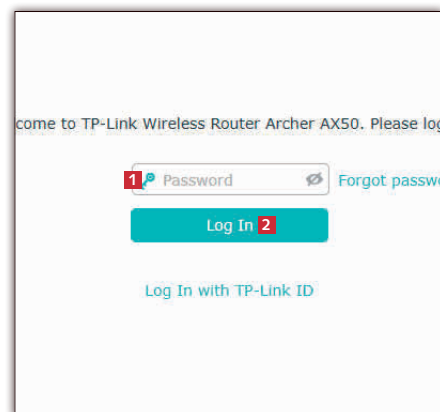
På administrasjonssidene til de respektive enhetene ser du som regel når den siste fastvareversjonen ble installert. Er det mer enn fem år siden, bør du vurdere å bytte ut utstyret for å redusere angrepsfaren. Her har vi en ruter fra TP-Link som eksempel.



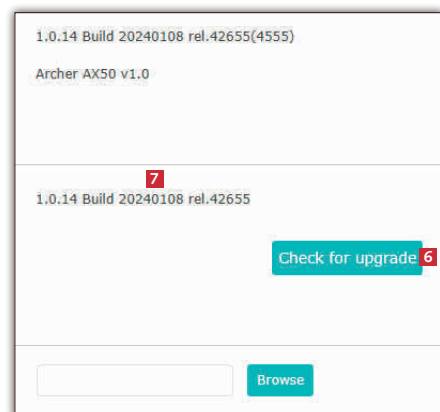
2 På en del enheter må du først klikke på **Advanced** **3** for å se detaljer om den installerte fastvaren.



3 Klikk på **System Tools** **4** eller lignende, og velg **Firmware Upgrade** **5**.



1 Finn adressen til enheten i Advanced IP Scanner – her er det en ruter. Skriv adressen i nettleseren, og trykk på **Enter**. Oppgi passordet til enheten **1**, og klikk på **Log in** **2**.



4 Klikk på **Check for upgrade** **6**. Du kan ofte se datoen for den nyeste fastvaren **7**. Er den fra før 2020, er det lite trolig at det kommer flere oppdateringer.

Du bør vurdere å kvitte deg med utdatert utstyr

Det er etter hvert 10–15 år siden smartheter til blant annet overvåking og kontroll av lys og varme begynte å dukke opp, og derfor er mye av dagens utstyr så gammelt at produsentene har sluttet å oppdatere det. Slik kan det selvfølgelig også være for enhetene dine. Det er utrolig hvor fort tiden går.

Dessverre er mange av sårbarhetene så dyptgripende at problemet kun lar seg løse ved hjelp av helt ny fastvare fra produsenten. Derfor oppdateres særlig nyere utstyr fra kjente produsenter hver gang det oppdages nye sårbarheter. Annerledes er det med utstyr av eldre dato eller generiske Kina-produkter. Derfor har du i praksis bare to muligheter hvis noen av enhetene ikke lenger mottar oppda-

teringer: Du kan levere dem til gjenvinning og kjøpe nytt, eller koble enheten fra nettverk/internett og bruke den lokalt, hvis det er en mulighet.



Mange nettverkskameraer, som dette fra D-Link, får ikke lenger fastvareoppdateringer. Dermed tettes heller ikke eventuelle sikkerhetshull.

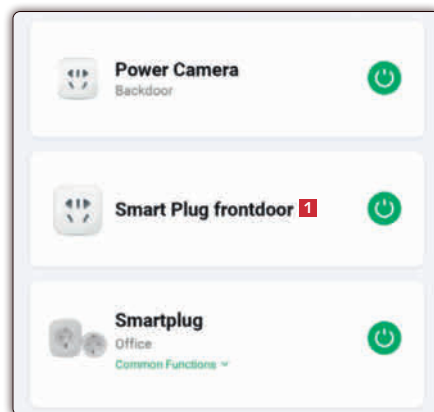


Har du en smarthøytaler, kan du oppleve at det for lengst er slutt på å laste ned sikkerhetsoppdateringer.

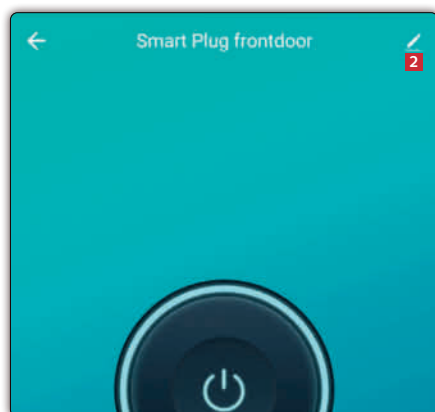


Oppdater enhetene via en app

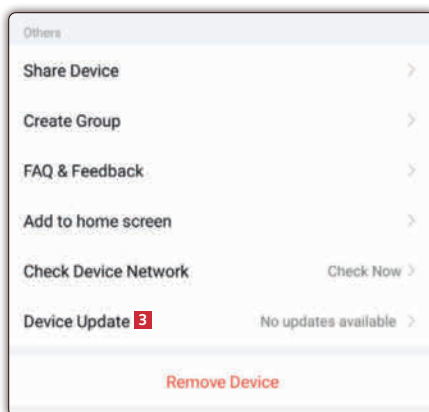
Mange av dagens smarthjemenheter kan kun styres fra en app på mobilen. Derfor kan det også være fra denne appen du må søke etter og installere eventuelle oppdateringer.



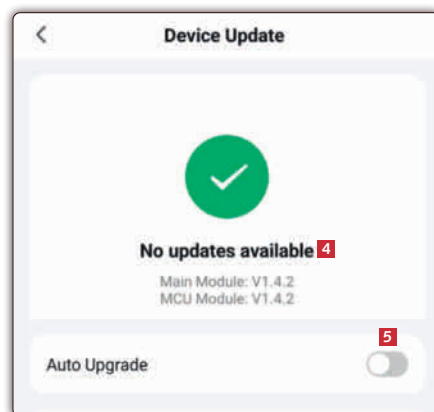
1 Hvis enheten kun kan styres fra mobilen, åpner du først den aktuelle appen. Hvis appen styrer flere enheter, trykker du først på den du vil oppdatere i oversikten **1**.



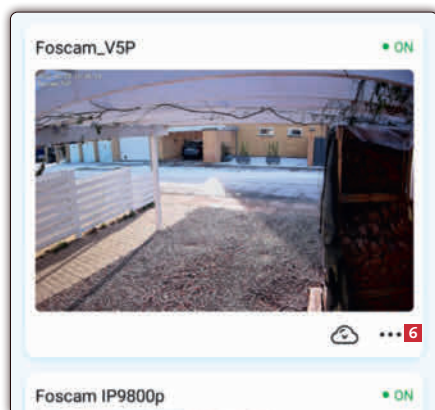
2 Trykk deg videre til enhetens innstillinger **2**.



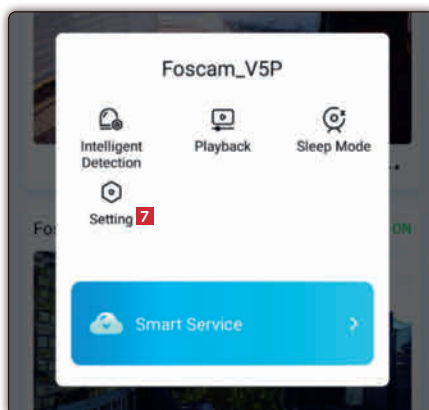
3 Trykk på **Device Update** **3** eller lignende.



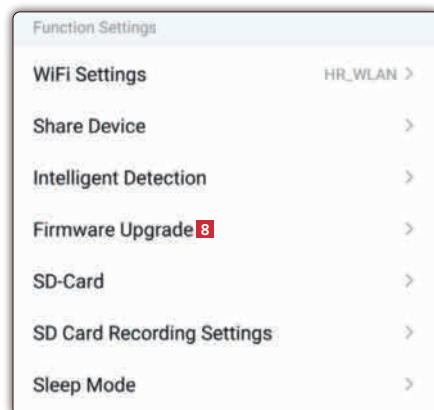
4 Her ser du om det finnes nye oppdateringer til enheten **4**. Ofte kan du også velge å la enheten laste ned og installere fremtidige oppdateringer automatisk **5**.



5 Hvis det er snakk om et app-styrt nettverkskamera, klikker du normalt på de tre prikkene under kamera-bildet **6**. Her er merket Foscam.



6 Deretter klikker du på **Setting** **7**.



7 Velg **Firmware Upgrade** **8**. Fra denne menyen kan du både oppdatere kameraet og sjekke når den siste oppdateringen ble installert.