Seniornett

Trygg på nett

Hva bør du vite om sikkerhet på nett

Seniornett

Innhold

Kapittel 1 - Sikkerhet og trygghet på nett

Sikkerhet og trygghet på nett er et vidt begrep og kan omfatte mye. Det å være trygg på nett er noe alle er opptatt av og ute etter.
Men alt for mange av oss går i fellen til de som ønsker å lure oss, nemlig svindlerne. De blir stadig mer avanserte og opptrer på stadig flere områder i vår digitale verden, de har blitt mer profesjonelle og er ganske kyniske.

Selv om dette høres nokså skummelt ut, kan du gjøre veldig mye selv for å minimalisere risikoen at også du blir offer for disse kriminelle.

I dette heftet vil vi komme med enkle råd. Vi håper at du vil gjør disse rådene til en del av din digitale hverdag. Kanskje blir du litt overrasket hvor enkle disse rådene er, og noen av rådene virker veldig opplagte. Men statistikk viser at mange ikke følger slike råd, selv om de kan virke opplagte.

Vi håper at du ved å følge disse rådene vil sørge for at du unngår økonomiske tap og timevis med "oppryddingsarbeid". Prisen er at ting kan ta noen sekunder lengre tid og at du føler du dobbeltsjekker flere ganger.

Sikkerhet og trygghet på nett har ikke bare med svindel og andre skumle ting å gjøre. Det innebærer også at du sikrer dine egne data, det vil si bilder, dokumenter, videoer, musikk, osv.

I dette heftet vil vi komme inn på de momentene som er viktig for å kunne minimalisere risikoen for at du blir offer for kriminell virksomhet og for å gi deg en trygg og fin digital hverdag.

Kapittel 2 - Beskytt mobilen

Din mobiltelefon er viktig i din digitale hverdag. Den må sikres slik at ikke andre kan misbruke den.

Det er fire ting du bør tenke på:

- Lås
- Hold den oppdatert
- Ha en plan for hva du gjør hvis den blir borte
- Bruk skytjenester

Lås

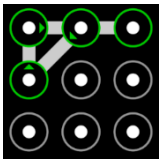
Mange har ikke lås på mobilen for å slippe det ekstra bryderiet det er å låse den opp hver gang du skal bruke den. Det er en risikabel strategi. Alle kan bli utsatt for svindel. Du kan miste telefonen eller den kan bli stjålet.

Det er flere ulike typer låser:

- Pin-kode
- Mønster
- Ansiktsgjenkjenning
- Fingeravtrykk

Det enkleste er ansiktsgjenkjenning. Da behøver du bare å se på mobilen, så låser den seg opp.
For fingeravtrykk kan du registrere flere fingre, slik at den kan brukes også hvis du har fått et sår på fingeren. Det er ikke alle mobiler som tilbyr ansiktsgjenkjenning eller fingeravtrykk. Vil du ha ansiktsgjenkjenning eller fingeravtrykk må du uansett også ha en pin-kode (det hender at den ikke gjenkjenner deg på ansikt eller finger).
Pin-kode er en (vanligvis) 4-sifret kode du velger som skal gis inn når telefonen er låst.

Mønster betyr at du, i en ramme med 9 prikker, skal tegne et mønster f.eks slik:



(Her er mønsteret fra prikk2 til 4 til 1 til 2 til 3)
Du velger altså et mønster som du klarer å huske. Du holder finger nede på skjermen mens du tegner mønsteret.

Det finnes innstillinger hvor du kan legge inn hvor lang tid mobilen skal være ubrukt før den låses. Her snakker vi om antall sekunder eller (noen få) minutter.

Hold mobilen oppdatert

Det å holde nettbrett og smarttelefoner oppdatert, dvs. både system-/programvareoppdateringer og oppdatering av de apper du bruker, er en av de beste sikkerhetstiltak du kan gjøre selv. I hver oppdatering ligger det en god del sikkerhetsoppdateringer, det vil si funksjoner som skal unngå at din mobil blir «infisert» av skadelig programvare.

De aller fleste av oss har satt som standard-innstilling at enheten skal oppdateres automatisk. Det er i og for seg et greit valg, bare man er klar over at jo eldre enheten du bruker er desto lenger må du vente på å få en oppdatering i den automatiske oppdatering.

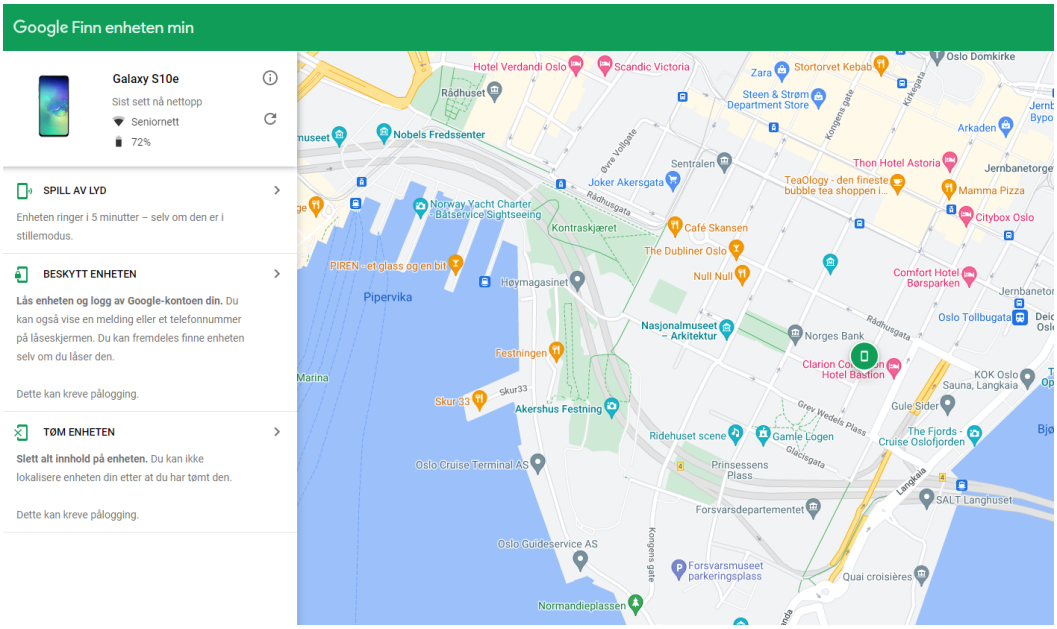
For å holde alle enheter du bruker oppdatert bør du selv regelmessig sjekke for oppdateringer manuelt. Du vil finne veiledere for oppdatering av programvare og apper i kapittel «Oppdateringer» i dette heftet.

Ha en plan for hva du gjør dersom mobilen blir stjålet eller mistet

Undersøk på forhånd hvordan du sporer din mobil. Dersom den er på og er koblet til internett, kan du fra en PC se hvor mobilen din er.

- For android-telefon gjør du dette ved å gå inn på https://www.google.com/android/find
  Har du ikke logget deg inn med din google-konto vil du bli bedt om å gjøre det.
- For iPhone logger du deg inn på iCloud og går du inn på https://www.icloud.com/find
  Her må du sørge for at «Finn enhet» er slått på

Her er et eksempel på hvordan det ser ut for Android:



Man ser hvor telefonen er (det grønne symbolet i kartet) og du ser at det er 3 ulike ting du kan gjøre:

- **Spill av lyd**
  Da vil telefonen «ule» i 5 minutter. Kjekt å gjøre når du eller din hjelper er i nærheten og skal finne den
- **Beskytt enheten**
  Da blir den låst og avlogget slik at andre ikke kan bruke den
- **Tøm enheten**
  Da fjernes alt på telefonen og den tilbakestilles til fabrikk innstillinger

Dersom du har slått av mobildata vil dette ikke virke. Derfor er det lurt å ha den slått på alltid.

Bruk skytjenester

Det er enkelt og lurt å ta mange bilder. Men det er risikabelt å kun lagre dem på telefonen. Du kan miste telefonen, eller noe kan gå i stykker slik at den ikke lenger virker. Da er det veldig dumt å miste bildene dine. Hvis du bruker skytjeneste på bildene så vil bildene automatisk bli lagret «i skyen». Da kan du også se dem fra andre enheter (f.eks. på PC eller nettbrett). Hvis du har aktivert en skytjeneste på din mobil og du bytter mobil, så vil alle bildene fra den gamle telefonen automatisk bli overført til den nye telefonen. Smart!

De vanligste skytjenestene for bilder på mobil er Google Foto, iCloud, Dropbox.
Les mer om dette i kapittelet om skytjenester.

Kapittel 3 - ID-tyveri

Definisjon av ID-tyveri: «uberettiget bruk av både stjålet og fiktiv identitet, med forsett å oppnå en økonomisk vinning for seg selv eller andre, eller å påføre tap eller ulempe for andre». Poenget her er at noen er ute etter dine (sensitive) opplysninger for at de skal utgi seg for å være deg.

Hvordan kan det skje. Du blir lurt / svindlet gjennom:

- **Netthandel**
  En falsk nettbutikk. Du «kjøper» noe der, men de har ingen varer. Du oppgir kredittkortnummer når du «betaler»

- **Sosiale medier**
  Noen har opprettet en falsk profil og sender melding til dine «venner» og ber dem om å bli med på noe som gir økonomisk gevinst. Den som mottar, tror det er fra deg og går på limpinnen

- **Oppgi personopplysninger i telefon**
  Det ringer en person fra politiet som sier han skal stoppe noen som holder på å stjele penger fra din konto. Han ber deg oppgi fødselsnr og bankid-koder. Han er selvfølgelig ikke fra politiet (selv om telefonnr du ser tilsynelatende er fra politiet)

- **Papirer på avveie**
  Papirer med sensitive opplysninger bør makuleres eller brennes

- **Falske linker**
  Det er kanskje den vanligste årsaken. Du får en epost som frister med penger eller lykke. Du skal bare trykke på en link og fylle ut et skjema.

Hvordan forhindre at du blir rammet av id-tyveri

Det kanskje vanligste er at du får en melding eller oppringing som ser ut som om den kommer fra en seriøs avsender (f.eks. politiet, skatteetaten, microsoft). Husk at du aldri skal oppgi sensitive data i telefon fra bedrifter eller offentlige etater. Sensitive data er koder du har mottatt på tlf, fødselsnr, bank-id eller lignende. Ingen seriøse organisasjoner vil spørre om dette. Selv om den som ringer høres seriøs ut og sier at han kommer fra politiet og skal hjelpe deg skal du ikke oppgi sensitive data over telefon. De mest avanserte svindlere opptrer som om de er seriøse aktører. Pass på at du ikke blir lurt.

Er det en melding som inneholder en link («trykk her») så er det sannsynligvis svindlere. Alle seriøse avsendere vil be deg om å logge inn på deres nettsider istedenfor å sende deg en link. (En link er en tekst du kan trykke på som fører deg til en nettadresse. Ofte er link-teksten forkortet og består av en rekke tegn som ikke gi mening. Dette er bare en substitutt for den egentlige og lange nettadressen).

Får du en melding på sosiale medier som tilsynelatende er fra en du kjenner, så skal du heller ikke oppgi noen kode (f.eks. ber «vennen» din om en kode du fikk på tlf fordi han sier at du er med på et lotteri). Det er sannsynligvis ikke din venn, men en som gir seg ut for å være vedkommende.
Får du en litt rar melding fra en bekjent, kontakt vedkommende (i en annen kanal) og hør om hen virkelig har sendt den meldingen.

Symptomer på at du er rammet av id-tyveri

- Du mottar regninger for produkter du ikke har bestilt eller ikke kjenner til
- Du oppdager ukjente transaksjoner eller kjøp på kredittkortregningen din
  Det er derfor lurt at du følger med jevnlig på transaksjonene dine
- Du mottar bekreftelse på kreditt eller endring av kredittrammen din uten at du har spurt om dette
  Noen andre enn deg har bedt om å øke kredittrammen. Ta straks kontakt med kredittkortselskapet
- Du får varsel fra posten eller andre om at adresseendring er mottatt
  Prøv å finne ut hvem som har gjort det. Ta kontakt med de du fikk melding fra
- Du blir kontaktet på telefon eller brev om kjøp du ikke har gjort eller kjenner til
  Prøv å finne ut hva og hvordan
- Du mottar gjenpartsbrev etter *kredittsjekk* uten å forstå hvorfor.
  Hvis du ikke har søkt om lån eller bedt om faktura ved kjøp på nett, noe som krever *kredittvurdering*, bør du umiddelbart kontakte kredittvurderingsselskapet for å finne ut hvem som står bak
- Du mottar post du ikke forstår hvorfor du får, for eksempel en faktura, et avtaleforslag eller hentemelding for noe du ikke har bestilt
- Ta umiddelbart kontakt med den som har sendt deg dette for å undersøke saken

Kapittel 4 - Svindel

Svindel er et forsøk på å lure noen til å gi bort informasjon eller gjøre en handling som fører til tap av penger.

Svindel eller bedrageri har eksistert i alle år. Men i den moderne tid har svindelmetodene blitt mer og mer digitale ved bruk av stadig mer avanserte teknologiske metoder.
Ved å kunne gjenkjenne de forskjellige metoder, ved å bruke sunn fornuft og ved å «holde hodet kaldt» kan man være bedre forberedt for å unngå svindel.

De er 3 hovedmetoder du kan bli svindlet på:

- **Fristelse**
  Eksempel «Du er den heldig vinner av …….» -
  Hva gjør du? Slett meldingen uten å gjør noe mer med den. Du vinner nemlig ingenting.

- **Frykt**
  Du har mange trusler på din maskin, eller du må gjør noe veldig raskt (du må gjør noe NÅ, ellers er det for sent)
  Hva gjør du? Stopp opp – ta det med ro – ta deg tid til å tenke deg om

- **Tillit**
  Du får melding fra en du kjenner som ber deg om å gjøre noe. Men er det naturlig at du får denne meldingen? Ber den deg om å gjøre noe uventet? Er det virkelig en du kjenner som har sendt deg denne meldingen?
  Hva gjør du? Ikke svar på meldingen og ta direkte kontakt (ring) med den kjente du tror har sendt deg denne meldingen

Mesteparten av svindel kommer i bølger eller er sesongbestemt.
Et eksempel er Microsoft-svindelforsøk. Du blir oppringt av en såkalt medarbeider fra Microsoft som sier at de har oppdaget en trussel på din datamaskin. De sier at de kan hjelpe deg med å få fikset problemet. Dette er selvfølgelig ren svindel.
Denne Microsoft-svindelen er aktiv i en bestemt periode. Da blir det etter kort tid en del omtale om disse svindelforsøkene i media. Flere og flere blir mer oppmerksom på disse svindelforsøkene. Da blir det plutselig helt stille fra Microsoft-svindlerne og etter en stund forsvinner dette ut av tankene til folk. Etter en stund starter samme type svindelforsøk igjen og da med en større «treffsannsynlighet».
Et eksempel på sesongbestemt svindel er at det vil bli en enorm økning av falske SMS-er fra for eksempel Posten, PostNord eller DHL i desember måned. Det henger sammen med at mange bestille ting på nett i forbindelse med jul, og mange sitter og venter på at pakken kommer frem. Dette er perfekte forhold for svindlerne.

Det finnes flere måter som kriminelle bruker for å prøve å svindle andre:

- **Phishing**
  Dette er den mest brukte form for svindel. Phishing er det engelsk ord for «fiske». Dette er en form for internettbedrageri, som er basert på å «fiske ut» personlig informasjon fra den som skal svindles.
  Det kommer som regel i form av en e-post, en SMS eller et telefonanrop. Disse e-poster eller SMS-er inneholder da ofte et falskt vedlegg eller lenke. Lenken fører til nettsiden som tilsynelatende er nettsiden til en pålitelig bank eller nettbutikk, men som er en falsk nettside. Det handler ofte om at du har vunnet noe eller at du for eksempel kan løse et problem med bankkontoen din.
  Det skjer også via direkte anrop på telefon ved hjelp av såkalt spoofing-teknologi (se beskrivelse lenger nede). Det er en person som tilsynelatende ringer fra politi eller en annen instans som de fleste av oss har tillit til.
  Målet er å få tak (fiske ut) i personlige opplysninger som da kan misbrukes for å svindle deg

- **Whaling**
  Eksempel: en såkalt bekjent kontakter deg i form av en e-post, en SMS eller en melding på Messenger fordi han eller hun er i nød og ikke lenger har tilgang til pengene sine. Typisk at den såkalt bekjente er på ferie i utlandet og har blitt frastjålet både bankkort og pass. Han/hun trenger penger å komme seg tilbake til Norge og ber deg om hjelp. Dette er såkalte tigge-e-poster eller tigge-meldinger

- **SMiShing**
  Svindelmeldinger tilsendt på SMS, tilsvarende svindelforsøk som kommer på e-post. Disse meldingene inneholder som regel en lenke til en falsk nettside, samt argumenter for at du skal besøke siden som f.eks. et tilbud som virker for godt til å være sant

- **Wangiri**
  Betyr at det kommer et anrop fra et utenlandsk nummer som ringer kun én gang. Målet er at du skal ringe tilbake. Du ringer nemlig tilbake til et telefonnummer med veldig høy takst. Ofte er det en telefonsvarer eller lydfil i enden av det utenlandske høytakst-nummeret som skal holde samtalen i gang lengst mulig. Jo lenger du lytter desto større blir telefonregningen din og desto mere tjener svindlerne

- **Spoofing**
  Er en teknikk som gjør at svindlere kan utgi seg for å kontakte deg fra et norsk nummer (eller trygg IP-adresse). For å utføre spoofing på telefon bruker svindlerne en programvare som viser et annet nummer enn det originale nummeret de ringer fra. Dermed kan samtalen se ut som at den kommer fra et norsk nummer noe som ofte vekker mer tillit enn et utenlandsk.
  Det er ofte at nummeret som vises på din telefon ser ut til å komme fra en instans som vi normalt har stor tillit til som Politi, NAV, Skatteetaten eller lignende og gjerne som et fasttelefonnummer. Men det kan også vises som et (tilfeldig) norsk mobilnummer. Dersom mobilnummeret ditt skulle bli spoofet betyr det ikke at mobilen din har blitt hacket.
  Målet med spoofing er som regel å fiske ut informasjon fra deg som kan misbrukes til å svindle deg.

Hva kan du se etter for å unngå svindel

- Phishing gjøres vanligvis på vegne av banker, myndigheter, selskaper og abonnementstjenester, dvs. instanser/ting du stoler på. Sjekk avsender
- Du vil bli ofte bedt om å klikke på en lenke eller betalingsforespørsel
- Det haster!
- Det kan være språk- og stilfeil i meldingen
- E-postadressen ligner den til det falske selskapet, men er ofte litt annerledes. For eksempel skattteetaten.no (med en ekstra ‘t') eller ‘DNB-payment.no' (et domene som ikke tilhører DNB selv)
- Meldingen har merkelige vedlegg.
  Ikke klikk på disse, de kan inneholde virus

Råd for å unngå svindel

- Bruk sunn fornuft og ikke foreta deg noe før du har tatt god tid til å tenke deg godt om. Ikke la deg lure til å handle for raskt!
- Ikke ring tilbake hvis du ser at et ukjent nummer fra utlandet har ringt deg
- Ikke klikk på lenker du har mottatt fra ukjente nummer eller ukjent avsender
- Slett de e-poster og SMS-er som kommer fra totalt ukjente eller som ikke virker legitime
- Ikke last ned apper fra andre steder enn Google Play og App Store
- Oppgi aldri BankID-koden din til noen, selv ikke til politiet.
  Det er ingen andre enn deg som skal bruke den
- Vær veldig kritisk – husk at ingen profesjonelle aktører spør etter personlige opplysninger
- Kontakt banken din eller andre offentlige instanser via deres offisielle numre hvis du får en henvendelse du mistenker ikke er legitim.
  Husk at nummeret kan være såkalt spoofet. Bruk derfor ikke «ring tilbake»-funksjon, men slå inn nummeret selv
- De fleste smarttelefonene kan blokkere anrop fra plagsomme numre

Har du blitt offer av svindel?

- Anmeld svindel til politi
- Ta kontakt med banken din.
  Ta evt. kontakt med din teleoperatør om du har oppgitt ditt mobilnummeret til svindlerne
- Bytt passordet umiddelbart dersom du har oppgitt innloggingsdetaljer
- Hvis det plutselig dukker opp en ny app på enheten som er ukjent for deg, slett den.

Kapittel 5 - Oppdateringer

Det å holde alle enheter du bruker oppdatert, dvs. både system-/programvareoppdateringer og oppdatering av de apper man bruker er en av de beste sikkerhetstiltak man kan gjøre selv.

De aller fleste av oss har satt som standardinnstilling, at enheten skal oppdateres automatisk. Det er i og for seg et greit valg, men man må være klar over at jo eldre enheten du bruker er desto lenger må man vente på å få en oppdatering i den automatiske oppdatering.

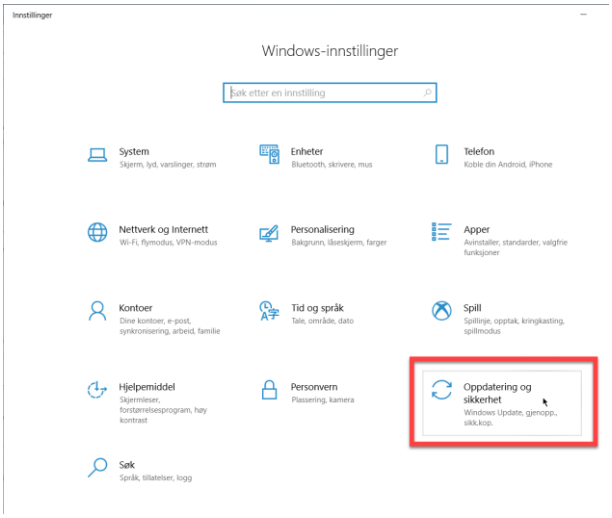
For å holde alle enheter du bruker til enhver tid oppdatert bør du selv regelmessig sjekke for oppdateringer manuelt.

Det gjør du slik:

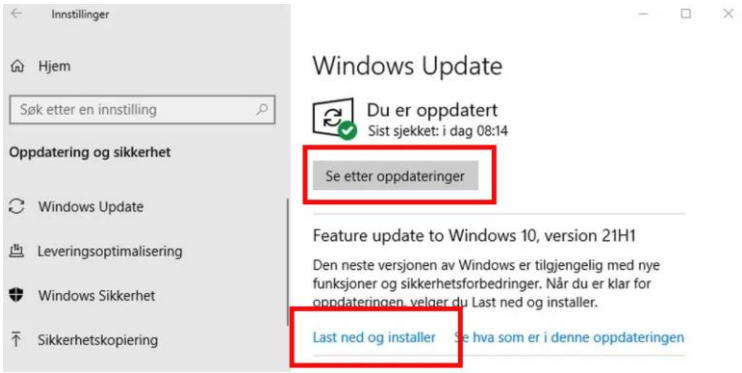
Oppdatering med Windows 10

1. Trykk på Startknappen (nederst til venstre) og trykk på Innstillinger (tannhjul-symbolet)

2. Velg «Oppdatering og sikkerhet»



3. Trykk på «Se etter oppdateringer». Det vises enten «Du er oppdatert» eller så vises en oppdatering som er tilgjengelig. Da kan du trykke på «Last ned og installer»

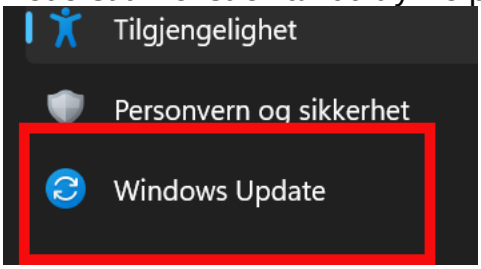


Oppdatering PC med Windows 11

1. Trykk på Startknappen som er ikonet som står lengst til venstre nederst på skjermen

2. Trykk på Tannhjul-ikonet (Innstillinger)

3. Nederst til venstre kan du trykke på Windows Update

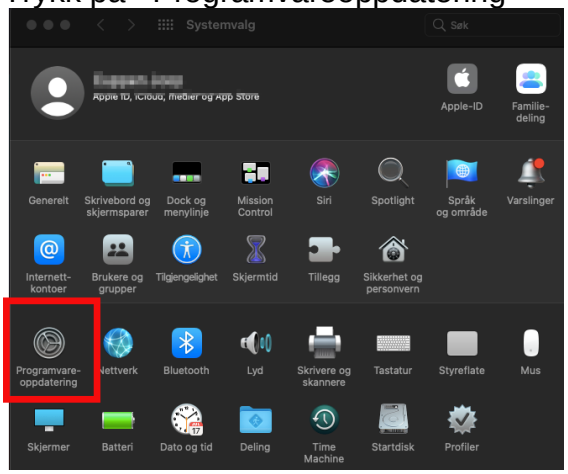


4. Trykk på «Se etter oppdateringer». Da vil det vises enten «Du er oppdatert» eller så vil en oppdatering som er tilgjengelig vises. De fleste oppdateringer vil lastes ned og installeres automatisk. For noen større oppdateringer vil du blir bedt om å starte PC-en på nytt

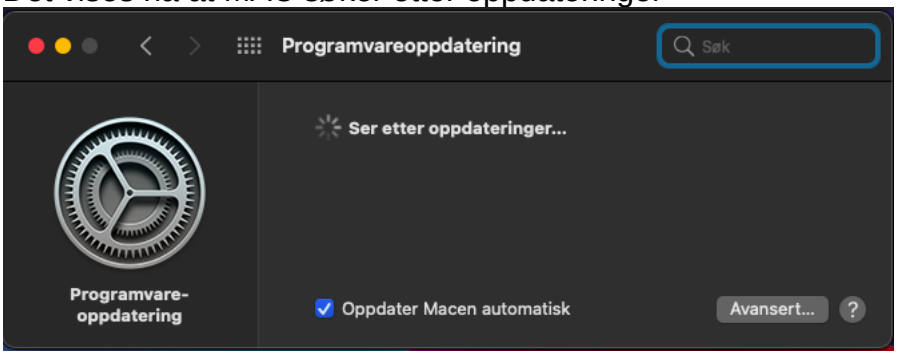
Oppdatering av Mac

1. Trykk på Tannhjul-symbolet, som du finner nederst på skjermen på det såkalte Dock

2. Trykk på «Programvareoppdatering»



3. Det vises nå at MAC søker etter oppdateringer



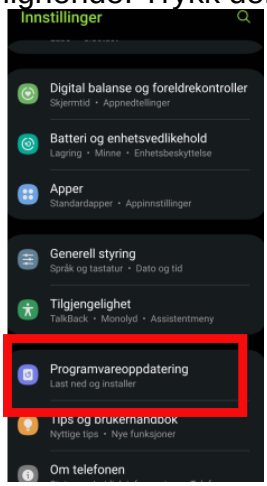
4. Om det er en oppdatering tilgjengelig vil den vises og du vil kunne velge «Oppgrader nå».
   Om det ikke finnes en tilgjengelig oppdatering, vil det vises at macOS er oppdatert og hvilken versjon som gjelder

Oppdatering Android nettbrett eller smarttelefon

Det mange forskjellige typer Android enheter. Det kan være Samsung, Huawei, OnePlus, Motorola osv. Alle har et litt ulikt utseende under «Innstillinger», men framgangsmåte for oppdateringer er ganske like for alle.

1. Trykk på Innstillinger (Tannhjul-symbolet)

2. Rull ned til du finner enten «Programvareoppdateringer», «Systemoppdateringer», «System og programoppdateringer» eller noe lignende. Trykk der.

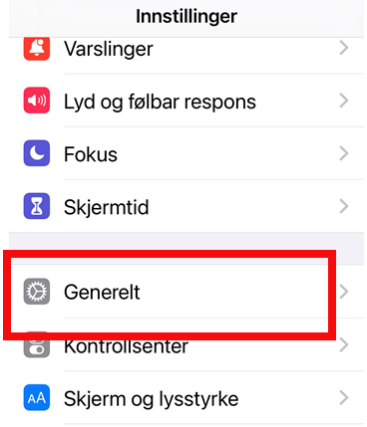


3. Noen Android enheter vil nå automatisk begynne å søke etter nye oppdateringer.
   For Samsung enheter må du trykke på «Last ned og installer». Om det er en oppdatering som er tilgjengelig vil den nå vises, og vil lastes ned og installeres. Om det ikke er en oppdatering tilgjengelig vil det stå «Programvaren (eller systemet) er oppdatert»

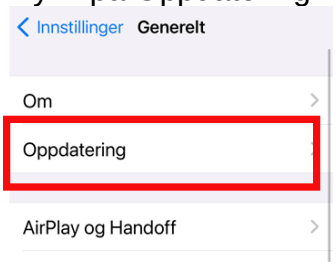
Oppdatering iPad eller iPhone

1. Trykk på Innstillinger (Tannhjul-symbolet)

2. Rull litt ned til du ser Generelt på venstre side. Trykk på Generelt



3. Trykk på Oppdatering

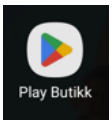


4. Det søkes nå etter en oppdatering som er tilgjengelig. Om det ikke finnes en ny oppdatering som er tilgjengelig vises følgende beskjed «iPadOS er oppdatert» eller «iPhoneOS er oppdatert» samtidig som det vises navn på siste oppdatering for eksempel iPadOS 16.1.1.
   Om det er en oppdatering er tilgjengelig vil du kunne velge «Last ned og installer»

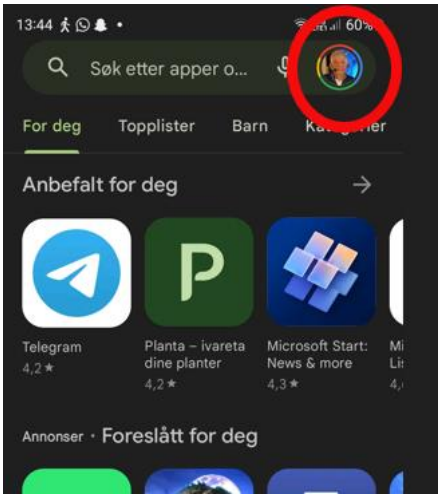
Oppdateringer av apper på smarttelefon eller nettbrett

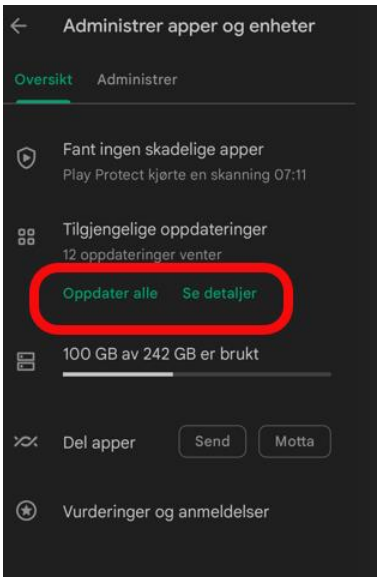
For Android

1. Trykk på Play Butikk / Google Play ikonet



2. Trykk øverst til høyre på profilbilde eller initialen din





3. Trykk på administrer apper og enheter. Under tilgjengelige oppdateringer vil du se om det er noen oppdateringer tilgjengelig. I dette tilfelle venter 12 oppdateringer på å bli installert, selv om automatisk oppdatering er slått på. Ved å trykke på «Oppdater alle» vil apper bli oppdatert der og da, og ikke når funksjonen «automatisk oppdatering» bestemmer seg for å oppdatere

For Apple (iPhone/iPad)

1. Trykk på App Store ikonet

2. Trykk på initialene dine øverst til høyre

3. Rull (scroll) litt ned til du finner «Kommende autooppdateringer».
   I dette tilfelle venter 8 oppdateringer på å bli installert, selv om automatisk oppdatering er slått på. Ved å trykke på «Oppdater alle» vil apper bli oppdatert der og da, og ikke når funksjonen «automatisk oppdatering» bestemmer seg for å oppdatere.

Oppsummering

Det er altså viktig at du regelmessig kontrollerer manuelt, om det finnes oppdateringer for enten programvare/systemet eller apper.
Dette for å ha den best tilgjengelige sikkerheten for din enhet, til enhver tid.

Kapittel 6 - Passord

Først noen enkle regler om passord:

- Lag gjerne et system der du kan konstruere sterke passord som ser helt «tilfeldig» ut men som du kan huske.
  Passord skal altså være lett å huske, men samtidig vanskelig å gjette for andre
- Lag gode passord med rett kombinasjon av tegn.
  Et godt og sterkt passord er en kombinasjon av store og små bokstaver, tall og spesialtegn som @, £, $, % eller mellomrom
- Et sterkt og sikkert passord består av minimum 8 tegn
  Hvert ekstra tegn gjør den sterkere
- Pass på at passordet ikke er (deler av) et vanlig navn etterfølgt av en fødselsdato
- Bruk aldri en hel rad av de samme tegnene på rad
  For eksempel 123456, AAAAAA, ABC123
- Vurder om du vil begynne å bruke en såkalt passordmanager
  Det er et program som tar vare på alle dine passord

Men hvorfor bruker de fleste av oss ikke disse reglene?

Passord er en utfordring for mange av oss. De fleste av oss har en betydelig mengde kontoer/påloggінger der vi skal lage og bruke et passord. Erfaringer tilsier at det er en utfordring å holde oversikt over alle kontoer vi har og mange tror at de bare har noen få.

Det er viktig å holde en viss oversikt over alle de kontoer vi har for å kunne styre og sikre disse godt nok. Eksempler på plasser der man muligens har opprettet en konto: Microsoft, Apple, Google, Facebook, andre sosiale medier, nettavisen, tele-operatør, TV-operatør, flyselskaper, hotell(bookinger), strømming (Netflix m.m.), nettbutikker, avisen, e-post program, parkeringsselskap, treningsstudio, Posten, Digipost, diverse programmer eller apper på de enheter vi bruker, Zoom/Teams/Skype, hjemlevering av mat, bensinstasjoner, leiebilselskap, El-butikker, konto for frivillig arbeid eller evt. jobbkonto.

Kjenner du deg igjen?

Mange vil kjenne seg igjen, og det er samtidig den store utfordringen. For å kunne huske passord til alle de nettsteder lager man typisk bare noen få enkle passord og bruker disse på flere forskjellige plasser.
En annen utfordring er at svært mange bruker funksjonen der programmet (for eksempel Facebook) «husker ditt passord» slik at du ikke trenger å logge deg inn hver gang du bruker programmet. Når man en sjelden gang må logge seg inn så husker man ikke passordet og må be om nytt passord. Det kan lage «rot i systemet».

For å få bukt med alle de passordproblemer mange opplever kan det være fornuftig å vurdere å ta i bruk et godt hjelpemiddel som kan oppbevare alle dine passord, nemlig en passordhåndterer. Fordelen av et slikt program er:

- Du trenger bare å huske ett passord
  Nemlig ved innlogging til passordprogrammet
- Alle dine passord blir oppbevart i programmet
  Dette gjør at du kan lage så mange forskjellige gode sterke passord som du trenger.
  I prinsipp et nytt sterkt passord for hver konto du har
- Du kan lage nye gode og sterke passord til alle påloggingerDette sikrer hver enkelt konto

Et av de passordprogrammene er LastPass. Dette er et program som er lett å skjønne og lett å bruke.
Seniornett har skrevet to artikler om dette programmet, som beskriver hvordan du kan laste ned programmet og hvordan du tar det i bruk. Du finner de artiklene her:
https://www.seniornett.no/ukens-app-er-lastpass-copy/
https://www.seniornett.no/ukens-app-lastpass-del-2/

Totrinns verifisering

I tillegg til brukernavn og passord, er det sterkt å anbefale at du bruker en ekstra sikkerhet ved innlogging. Dette kalles totrinnsverifisering, totrinnsbekreftelse eller tofaktorautentisering.
Det gjør kontoen din sikrere fordi det hindrer andre å logge inn på din konto selv om uvedkommende kjenner til ditt passord.

Totrinnsverifisering fungerer slik:
Etter at du har skrevet inn brukernavn og passord og har trykt på «Logg inn» må du bruke noe annet (f.eks. smarttelefon) som ekstra nøkkel. Enten får du tilsendt en kode som du må skrive inn på innloggingsbildet eller du må bekrefte via en app på din smarttelefon. Måten koden sendes på kan være via SMS eller en App.

Med andre ord: Du logger du inn med noe du vet (brukernavn og passord) og noe du får (den tilsendte koden eller bekrefte i app-en). Passordet er altså 1.nøkkel, mobilen er 2. nøkkel
De fleste vil kjenne igjen denne måten av innlogging fra innlogging i banken. Først skrive inn fødselsnummeret (1.nøkkel). Deretter skrive inn kode fra kodebrikke og ditt personlige passord (2.nøkkel). Den andre nøkkel kan også være BankID app på telefon.

Hvordan kan du aktivere totrinnsverifisering for forskjellige kontoer/nettsteder?
Det er ikke nettsteder som tilbyr totrinnsverifisering men det er mulig for noen av de viktigste kontoer mange av oss bruker. I tillegg er det forskjellige framgangsmåter for de forskjellige kontoer der du kan aktivere totrinnsverifisering for.

Enkle og instruktive veiledninger hvordan du kan aktivere totrinnsverifisering for forskjellige kontoer finner du på nettsiden til nettvett.no: https://nettvett.no/2-trinns-bekreftelse/

Men du kan selvfølgelig også ringe Seniornetts datahjelp på telefon 22 42 96 26, om du trenger hjelp til å komme i gang med denne totrinnsverifiseringen.

Det er viktig at du aktiverer totrinnsbekreftelse for alle de kontoer der det er mulig!!

Kapittel 7 - Skytjenester

Å abonnere på én eller flere skytjenester betyr at en kopi av dataene dine lagres et sentralt sted. Du har dermed sikkerhet for at data ikke blir borte selv om du skulle miste din enhet (pc/brett/telefon), enheten blir ødelagt eller når du bytter enhet. Skytjenestene er laget slik at de automatisk kopierer dine data straks de er opprettet eller endret. Du behøver derfor ikke å tenke på sikkerhetskopier når du først har startet med en skytjeneste.

For at en skytjeneste skal fungere må du være koblet til internett. Tar du bilder uten å være på nettet så vil systemet synkronisere bildene (altså laste dem opp til «skyen») når du får internett-forbindelse igjen. Du behøver dermed ikke å være konstant på nettet.

Du behøver heller ikke å tenke på hvor dataene blir lagret. Dine data er uansett alltid tilgjengelig for deg (du må ha logget på med brukernavn, passord og evt. to-trinns pålogging)

Stort sett så logger man på skytjenesten én gang for hver enhet du bruker. Så når du har opprettet en konto og logget deg på via din tlf så trenger du ikke å tenke noe mer på dette. Alt går automatisk og du trenger normalt ikke å logge på igjen (telefonen eller annen enhet husker din pålogging)

Hvor mye koster det

De fleste skytjenester har noe gratis og noe som koster. Det som bestemmer prisen er hvor mye data du lagrer. Husk at videoer bruker mye lagringsplass, mens dokumenter og bilder kan variere i størrelse. Typisk for skytjenestene er at det første nivået av lagringsplass er gratis. Så betaler du hvis du vil ha mere plass.

Hvordan virker det

Det er vanligvis 3 ulike områder man bruker skytjenester:

- Epost
- Bilder
- Dokumenter

De fleste oppfatter ikke Epost som en skytjeneste, men det er det i de fleste tilfeller. Det betyr at du kan se epostene dine på flere enheter (hvis du skriver en epost på PC vil du straks etterpå se den samme på epostprogrammet på din telefon). Dette betyr altså at de epostene du ser på din enhet er bare en kopi av selve epostene (som da ligger lagret sentralt).

De største skytjenestene tilbyr gjerne alle tre områdene. Plassen du bruker er da summen av Epost, bilder og dokumenter.

Husk at Dokumenter her er alle typer filer du jobber med. Det kan være regneark, presentasjoner, skrevne dokumenter ol.

Epost tar ofte mye plass, spesielt hvis man ikke sletter gamle meldinger. Husk at alt du sender også lagres. Det er derfor lurt å slette gamle sendte meldinger for å spare plass. Ha det som en regel at du sletter eposter fortløpende (eller lagrer i mapper de du trenger å ta vare på)

Den kanskje viktigste skytjenesten er den du legger inn på din mobiltelefon som håndterer **bilder**. Det betyr at hver gang du tar et bilde så kopieres dette opp «i skyen». Du merker ikke at det skjer og du trenger ikke å tenke på hvordan det skjer. Det som er fint er at alle bildene du tar automatisk blir tatt vare på selv om du mister telefonen eller skal bytte til en ny.

På en PC/Mac hvor du har skytjeneste installert vil det fungere slik at hver gang du oppretter eller endret et **dokument** (og et dokument kan være hva som helst) så kopieres dokumentet opp «i skyen». Det betyr at du kan fortsette å redigere dokumentet på en annen enhet. Dette er spesielt nyttig når du anskaffer deg en ny pc. Når du logger inn i skytjenesten på den nye pc (og det gjør du kun én gang) så dukker alle dokumentene fra den gamle pc opp i den nye. Du behøver altså ikke lenger å tenke på å ta sikkerhetskopi av dokumentene dine. Det skjer automatisk.

For flere av skytjenestene er det også mulig å dele dokumentene. Det vil si at flere personer får tilgang, og når én person da legger inn et dokument så får alle de andre automatisk kopi av dokumentet. Dette kan være svært nyttig for foreninger og lag. Men husk da på at alle som har tilgang til dokumentet må bruke av «sin» lagringsplass. Og den som deler mappen med felles-dokumenter bør tenke på om alle andre også skal kunne endre og slette dokumentene.
Et eksempel er et kor som har alle notene sine i en delt mappe på en skytjeneste. Alle i koret kan både endre og slette. Så slutter et kormedlem og han sletter da alle notene (de trenger han jo ikke lenger). Dermed blir alle notene slettet for alle andre kormedlemmer også. Her må man altså passe på hvem som har tilgang til hva. Det er fornuftig at kun noen få personer kan slette dokumenter på fellesområdet.

Hva må du passe på

Det er som sagt alltid en grense for hvor mye data du kan lagre i de ulike skytjenestene. Grensen for hva som er gratis varierer og prisen på ekstra lagringsplass varierer også. Noen medregner plassen din epost tar i den totale lagringsplassen. Det er derfor lurt å følge litt med på hvor mye av lagringsplassen du har brukt. Det er gjerne mange dokumenter og bilder du ikke lenger har bruk for. Logg deg da på skytjenesten (eller gå inn på det området der filene ligger) og fjern det du ikke trenger. Da holder du forbrukt lagringsplass nede.

Hvilke skytjenester finnes

Det finnes mange. For bilder fra telefon er de to vanligste Apple iCloud og Google foto. Har du iPhone vil iCloud allerede være installert. Tilsvarende for android-telefon vil (vanligvis) Google foto være installert. Gå inn på appen og aktiver (du må alltid først logge på med apple-id eller Google-id, men normalt trenger du kun å logge på én gang)

De mest populære tjenestene på privatmarkedet tilbyr sikker og trygg lagring av bilder, videoer og filer – blant de største finner du disse (hvor mye lagringsplass som er gratis er slik pr høsten 2022. Dette kan fort endres):

Min Sky: Telenors skylagringstjeneste, som gir deg ubegrenset lagring av bilder og videoer – dette er inkludert i mobilabonnementet fra Telenor

iCloud: Apples skylagringstjeneste, som de fleste iPhone- og iPad-eiere har vært innom. Brukes til å ta sikkerhetskopi, samt lagring av bilder og videoer. Du har 5 GB gratis

Google: Her ligger dokumentlagring, bildelagring og epost. Har du gmail-epost er dette inkludert. Du har 15 GB gratis.

Dropbox: Dette er en av de første og største skylagringstjenestene som står på egne ben. Har svært mange brukere, og et godt system for blant annet deling av filer. 2GB er gratis, men det finnes ordninger der du får mer plass uten å betale.

OneDrive: Microsofts skylagringstjeneste, som er tett integrert med både Windows og Office-løsninger. Logger du på din PC med en epost-adresse, da er dette en Microsoft-konto og du har OneDrive inkludert. Du får 5GB gratis

Jottacloud: En norsk utfordrer, som blant annet har slått seg opp med en god løsning for sikkerhetskopiering av datamaskiner til skyen. 5 GB er gratis

Hvordan installerer du en skytjeneste

Søk opp ulike skytjenester via en nettleser. Når du har bestemt deg, gå inn på tjenestens nettside og opprett en konto. Gjelder det mobiltelefon eller nettbrett, last ned app-en fra Google Play butikk eller Apple app-store. Gjelder det PC/Mac, last ned programmet fra skytjenestens nettside.

Når du starter opp programmet eller app-en, må du logge deg på. Det gjøres normalt kun én gang. Og da er du i gang og kan lene deg tilbake og vite at dine data er trygge.

Var det vanskelig? Kontakt datahjelpen på Seniornett. Vi hjelper deg!

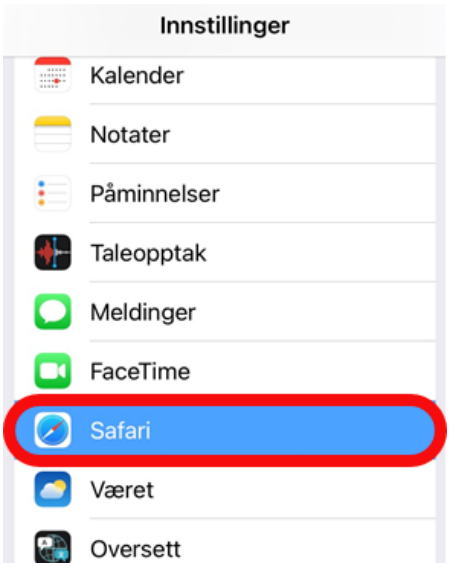
Kapittel 8 - Sikker surfing

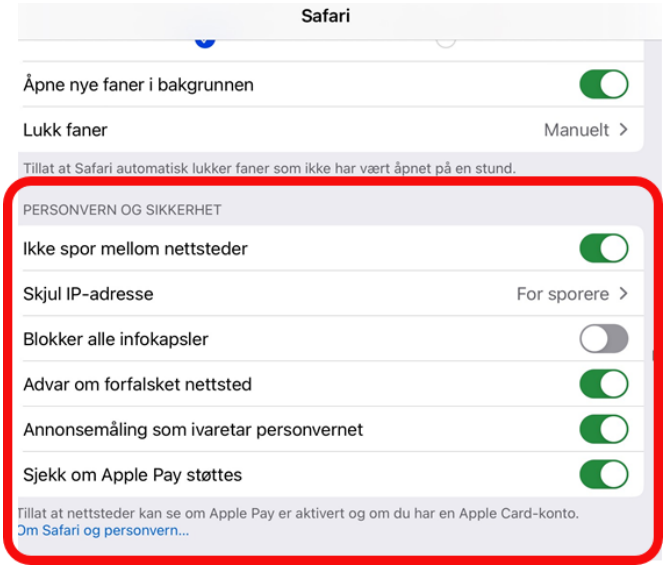
For å kunne bruke internett trenger du en nettleser.
De mest kjente nettlesere er Safari (for iPhone, iPad og Mac), Google Chrome og Edge.

Du kan øke sikkerheten i Safari ved å aktivere noen innstillinger. Det gjør du slik for iPad og iPhone:

1. Åpne Innstillinger (Tannhjulsymbolet)
   

2. Rull (scroll) ned til du finner Safari til venstre, og trykk på Safari. Til høyre vil du nå se en del valg. Rull ned til du finner delen «Personvern og sikkerhet». Slå på alle funksjoner der, kanskje med unntak av «Blokker alle infokapsler», fordi den kan skape problemer med å få tilgang til vise nettsteder.

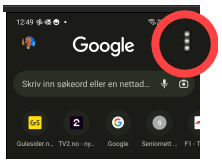




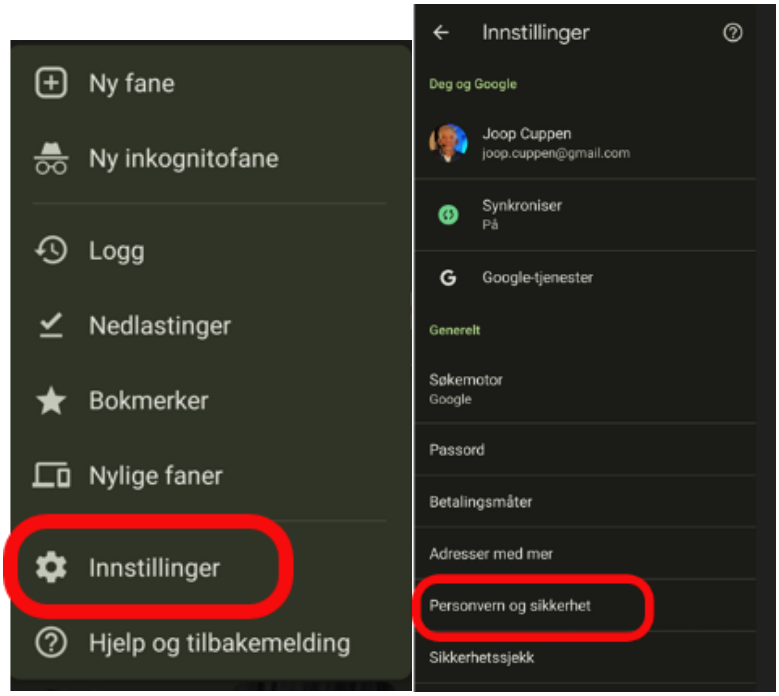
For Google Chrome, som brukes både på PC, Android-enheter (telefon og nettbrett) og IOS-enheter (iPhone, iPad, Mac), gjør du slik:

1. Åpne Google Chrome

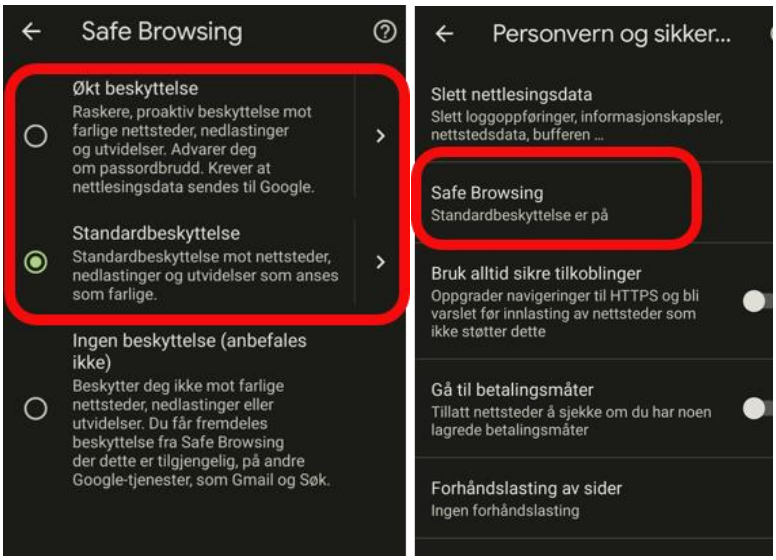
2. Trykk på de tre prikker, øverst til høyre



Velg Innstillinger og deretter Personvern og sikkerhet



3. Trykk nå på Safe Browsing og velg deretter nivået du ønsker. Standardbeskyttelse anbefales som minimum beskyttelse. Men du kan også velge den høyeste beskyttelse som heter Økt beskyttelse.



Standardbeskyttelse

- Oppdager og advarer deg om farlige hendelser idet de inntreffer
- Kontrollerer nettadresser opp mot en liste i Chrome over utrygge nettsteder
- Få en advarsel hvis passordet blir avdekket i datainnbrudd

Økt beskyttelse

- Forutser og advarer deg om farlige hendelser før de inntreffer
- Holder deg trygg i Chrome og kan brukes til å øke sikkerheten din i andre Google-apper
- Øker sikkerheten for deg på nettet
- Gir deg en advarsel hvis passordet blir avdekket i datainnbrudd
- Sender nettadresser til Safe Browsing for å sjekke dem

Kapittel 9 - Oppsummering

1. **Bruk sunn fornuft og ta det litt ekstra tid til å sjekke**
   Dersom det dukker opp noe du er i det minste tvil om det er svindel eller ikke, vil blant annet et raskt søk på nett etter deler av teksten i meldingen kunne avsløre svindelen.
   Bruk altså litt ekstra tid for å sikre deg.

2. **Er det for godt til å være sant, så er det nok det**
   Med dette ordtaket vil man i utgangspunktet kunne avsløre mange type svindel.
   Vær derfor ekstra skeptisk til tilbud som avviker for mye fra det andre kan tilby. En svært stor andel av disse tilbudene er nemlig for godt til å være sant, altså svindel.

3. **Du vinner ikke noe**
   «Du kan vinne en gratis iPhone, om du bare svarer på noen spørsmål». Eller så får du en melding eller e-post at du allerede er trukket ut som vinner av en premie. Dette virker kanskje kjent for mange. Da blir mange fristet til å gi fra seg personlig informasjon, og til og med betalingskortinformasjon for å dekke frakten av premien de har vunnet. Ja, det er veldig fristende med konkurranse der man med minimal innsats har en mulighet til å vinne en flott premie. Dessverre er det overhode ingen som vinner noen ting. Den eneste som vinner er den som er svindler.
   Selv om vi ikke kan si at alle konkurranser er svindel, bør man unngå konkurranser, fordi det er ekstremt vanskelig å skille ekte fra falske konkurranser.

4. **Hold alle enheter du har oppdatert**
   Oppdatering av alle enheter du bruker er en av de beste sikkerhetstiltak du kan gjøre selv. Oppdateringer tetter hullene i sikkerhetsnettet, som gjør at det er mer sikker å bruke enheten, spesielt når man går på nettet.
   Oppdateringer er altså viktig. Sjekk de regelmessig manuelt.

5. Ikke skam deg når du har blitt svindlet

Det å bli offer av svindel er litt skambelagt. Mer enn halvparten av befolkningen ville skamme seg hvis de ble et offer av nettsvindel.
Negative følelser av skam er oftere fortere forbundet med nettsvindel enn med tradisjonelle former for kriminalitet. Det er viktig å melde fra om datakriminalitet, og dele det med andre. Det å dele det med andre vil i de fleste tilfeller lette på den skamfølelse. Og det vil gi, blant annet myndighetene, en bedre innsikt hvor stort problemet er, for dermed kunne sette det enda mer på dagsorden.
Ikke skam deg, du er helt bestemt ikke alene. Dette skjer med flere hundre tusen mennesker hvert år i Norge.

6. Vær skeptisk men ikke engstelig

Selv om det er en del søkelys på alt det «skumle» som kan skje i den digitale verden, er det viktig å være skeptisk men ikke engstelig. Det å bruke alt digitaliseringen har gitt oss skal vi være glade for. Det gir oss mange muligheter til å oppleve mye glede, gode øyeblikk og et enklere liv. Med den kunnskapen du får fra dette heftet vil du kunne få en trygg digital hverdag.

7. Kommer dette fra den jeg tror det kommer fra?

Vær litt årvåken.
En kjent framgangsmåte for svindlere er at de utgir seg for å være en person du kjenner.
Dobbeltsjekk direkte med den kjente, om det er noe som virker litt rart eller unormalt.
Vær litt årvåken.

8. Ikke si: «det vil aldri skje meg»

Det heter at «alle som har en e-postadresse, mobilnummer eller konto på sosiale medier, er mulige ofre». Viktig er å nevne at dette med svindel er i de aller fleste tilfeller ikke mot deg personlig. Det er ofte tilfeldig at du blir utsatt for svindel. I noen tilfeller er det en bestemt liste de går etter men som regel er alt fullt automatisert og tilfeldig. Om du er bevisst på at du er like utsatt for svindelforsøk som alle andre vil det gjør det lettere å avsløre svindelforsøk.

9. Passord er en utfordring

Passord er for mange en utfordring. Det å lage gode og mange forskjellige passord har vist seg å være vanskelig for mange. Løsningen kan være å bruke et trygt og enkelt program som tar vare på alle dine passord. Husk også 2-trinns autentisering som er en «ekstra lås på døren» ved innlogging til forskjellige kontoer.

10. Generelle råd for å unngå svindel

Ikke ring tilbake hvis du ser at et ukjent nummer fra utlandet har ringt deg og ikke klikk på lenker du har mottatt fra et ukjent nummer.
Vær kritisk når en såkalt profesjonell aktør spør etter personlige opplysninger. Kontakt banken din via offisielle numre hvis du får en henvendelse du mistenker ikke er legitim. Og aldri oppgi BankID-koden din til noen, selv ikke til politiet.