100 effektive tips for bedre sikkerhet

Bruk av internett, mobil og pc medfører mengder av fallgruver. Her får du hundre omhyggelig utvalgte sikkerhetstips som gjør den digitale hverdagen langt tryggere – hvis du husker å følge dem.

Journalister
Martin Lorentsen
Henning Rasmussen

Det er dessverre ingen mangel på dårlige nyheter når temaet er hvordan vi bruker digitale hjelpemidler som pc og smarttelefon. I takt med at vi blir stadig mer avhengige av digitale enheter, blir svindlerne stadig mer iherdige og avanserte i forsøkene på å utnytte avhengigheten.

I dag utgjør angrepene på nettet en større trussel mot din og min hverdag enn noen gang tidligere. Med utbredelsen av kunstig intelligens har trenden forsterket seg ytterligere ved at yrkeskriminelle har fått et kraftfullt verktøy som gjør det mulig å automatisere den lyssky virksomheten.

Omfattende svindel

Vi har allerede sett utallige eksempler på at kunstig intelligens misbrukes til å forfalske videoer, etterligne stemmer og dikte opp tekster i den hensikt å lure intetanende ofre til å gi fra seg data som passord og betalingsinformasjon.

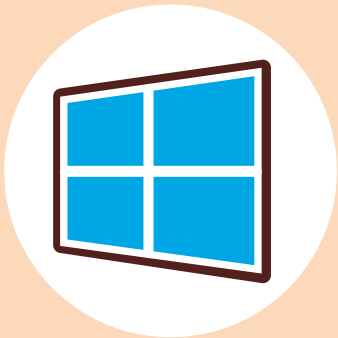
Men selv om den nye teknologien i økende grad utnyttes til nye former for svindel, legger ikke det noen demper på bruken av de gamle metodene. Identitetstyverier der Facebook-bilder og privat informasjon utnyttes til å opprette en falsk identitet, er ledd i en annen form for svindel som fortsatt er svært utbredt. På samme måte er det fremdeles mulig å kjøpe katta i sekken når du handler på nettet. Svindlerne har heller ikke sluttet å bombardere innboksen i e-postprogrammet med forsøk på nettfiske.

100 effektive sikkerhetstips

Dessverre ligger vi som ofre nesten alltid et skritt bak de kreative kriminelle. Likevel er det mye du kan gjøre selv for å redusere risikoen. Forutsetningen er at du vet hva du skal gjøre. Derfor får du her 100 effektive sikkerhetstips som gir optimal beskyttelse mot de aktuelle truslene.

Foto: ann1911, Dreamer Light, Design Squirrell/Shutterstock.com

E-post



Windows

Nettverk

Passord

Programmer

Mobil

Facebook

Nettleser

Netthandel

E-POST

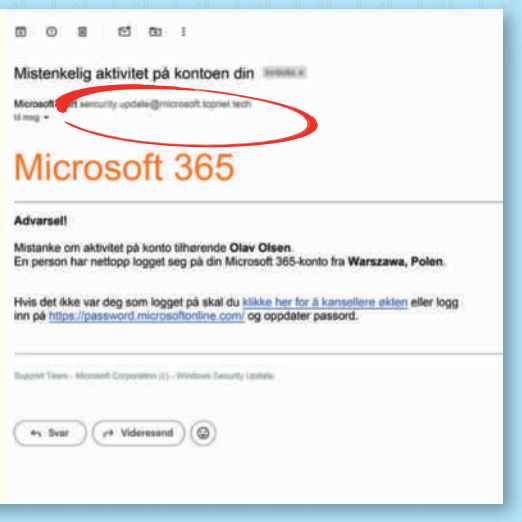
1
Lange og sterke passord

Den viktigste beskyttelsen mot at kriminelle misbruker e-post-kontoen din, er at du sikrer den med et godt passord. Hackere og svindlere forsøker hele tiden å få tilgang til e-postkontoer, men må gi tapt hvis passordet er tilstrekkelig langt og komplisert. Det kan du lese mer om på: **komputer.no/2513**

2
Sjekk avsenderen når du får e-post

De falske e-postene har etter vært blitt så troverdige at det ofte er ganske små detaljer som avslører at det dreier seg om svindel. Vær særlig oppmerksom på avsenderadressen.

Se nærmere på avsenderadressen. Den avslører ofte en annen avsender enn det som fremgår av meldingen.



E-post er ikke den beste kommunikasjonsformen hvis du har behov for å sende følsomme personopplysninger til myndigheter eller firmaer.

3
Ikke del alt via usikker e-post

Vanlig e-post blir ikke kryptert og er derfor en usikker kommunikasjonsform. Det betyr at du aldri må oppgi sensitiv informasjon som personnummer, kopi av passet ditt eller lignende i en e-post. I stedet bør du velge en løsning du vet er sikker.

4
La deg ikke lure av dyktige svindlere

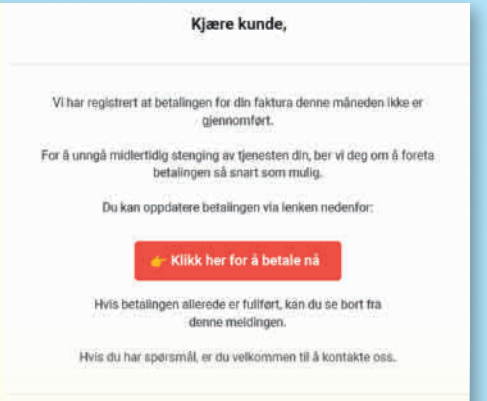
På engelsk kalles det "social engineering" når kriminelle lurer ofre til å tro at de har fått e-post fra en sønn eller datter som trenger øyeblikkelig økonomisk hjelp til å løse et problem. Det har svindlerne blitt så gode til at du alltid bør kontakte avsenderen direkte hvis noen skriver til deg og ber deg overføre penger eller sende dem personlig informasjon.

5
Krypter følsom informasjon i e-post

Vi advarer mot å bruke e-post til å sende personfølsom informasjon. Metoden er ganske enkelt ikke tilstrekkelig sikker. Hvis du sender e-post med annet innhold som du heller ikke vil risikere at havner i feil hender, bør du sjekke i innstillingene for e-postkontoen om det er mulig å kryptere innholdet ved hjelp av S/MIME. Alternativt kan du vurdere å sikre e-post-programmet med OpenPGP eller tilsvarende tjenester.

6
Klikk aldri på ukjente koblinger

Når du mottar e-post fra et firma, er ofte koblinger maskert som knapper eller bilder, og det kan være risikabelt å klikke på dem. Ved å holde musepekeren over knappen, kan du avsløre hvilken nettside knappen vil åpne. Det sikreste er likevel å aldri klikke på slike knapper.



I denne falske e-posten vil avsenderen ha deg til å klikke på den røde knappen, men den tar deg rett til en svindelside.

7

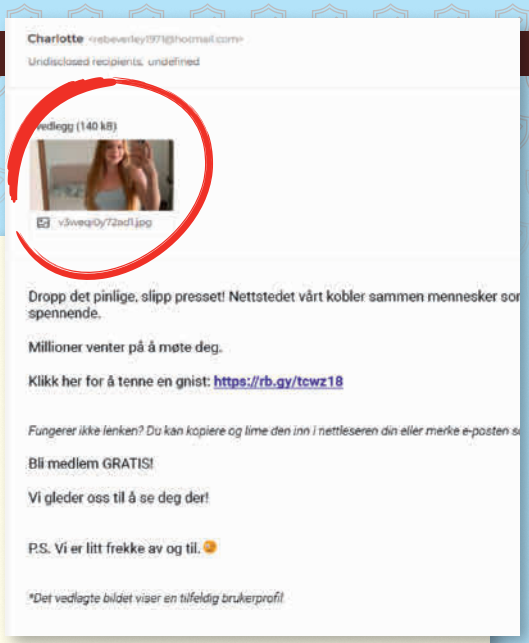
Bruk tofaktor-autentisering

De fleste e-posttjenester lar deg bruke den nye og sikre påloggingen som kalles tofaktorautentisering. Det virker på omtrent samme måte som med BankID, der du bruker et vanlig passord til første del av påloggingen. Deretter får du en engangskode på mobilen. Fremgangsmåten ser du her: **komputer.no/2513**

8

Unngå å åpne vedlagte filer

Når du mottar en skadelig e-post, inneholder den ofte en eller flere vedlagte filer. De fleste vet at det er farlig å kjøre programfiler som slutter på .exe, men det gjelder faktisk også for andre filtyper. De kriminelle har blitt så dyktige at selv vedlagte bildefiler kan utgjøre en trussel ved at de inneholder skadelig kode.



Det kan også være farlig å åpne bilder som er lagt ved i e-post.

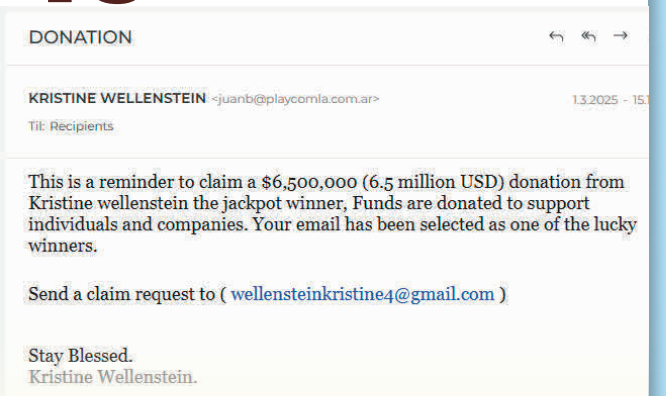
Språket i de falske e-postene er ofte resultatet av dårlig maskinoversettelse.

9

Avsenderens språk og tone

Hvis du handler på nettet, er det ikke uvanlig at man får e-post fra fraktselskaper som DHL eller GLS. Før du følger anvisningene i meldingen, bør du imidlertid ta en kritisk gjennomgang av språket. Dårlig oversetting er gjerne et varsko om ugler i mosen.

10



Tilbud om gratis penger er alltid fristende, men slikt finnes jo ikke på ordentlig og bør møtes med dyp mistenksomhet.

Vær skeptisk til ukjente avsendere

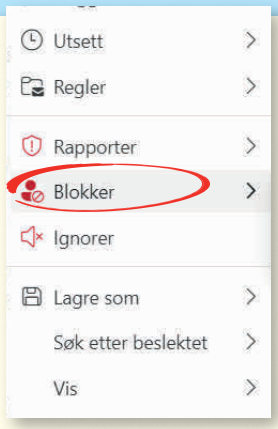
Det er som om vår menneskelige natur tilsier at en del av den medfødte skepsisen slås av, så lenge løftene er tilstrekkelig fagre og urealistiske. Nigerianske svindlere har for eksempel lenge hatt suksess med en svindel der de lurer ofrene til å tro at de – til alles store overraskelse – er begunstiget i testamentet til en søkkrik, men ukjent slektning.

Det er selvfølgelig fristende å tro på noe slikt, men hvis navnet på avsenderen er ukjent, fraråder vi på det sterkeste at du i det hele tatt innleder en dialog. Hvis du først begynner å svare på slik e-post, kan du raskt bli trukket inn i et farlig nettverk av løgner der du til slutt uansett ender med å være den som betaler.

11

Blokkering av uønsket e-post

Alle seriøse selskaper og organisasjoner som sender ut nyhetsbrev og annen e-post, gir mottakeren muligheten til når som helst å kansellere. Hvis du får uønsket e-post fra useriøse avsendere, kan du i stedet lage et filter i e-posttjenesten. På adressen under viser vi hvordan det gjøres i Gmail: **komputer.no/2513**

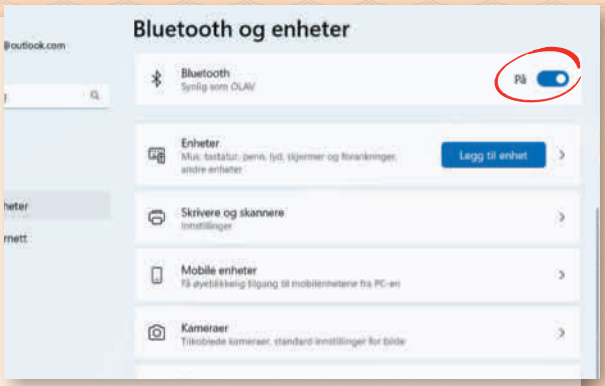


Får du e-post du ikke kan kansellere, kan du i stedet blokkere meldingene.

12

Slå av Bluetooth når funksjonen ikke er i bruk

Bluetooth er en fantastisk trådløs teknologi som lett kobler for eksempel et hodesett til pc eller mobil. Men den kan også utnyttes av kriminelle, så slå av Bluetooth når funksjonen ikke er i bruk.

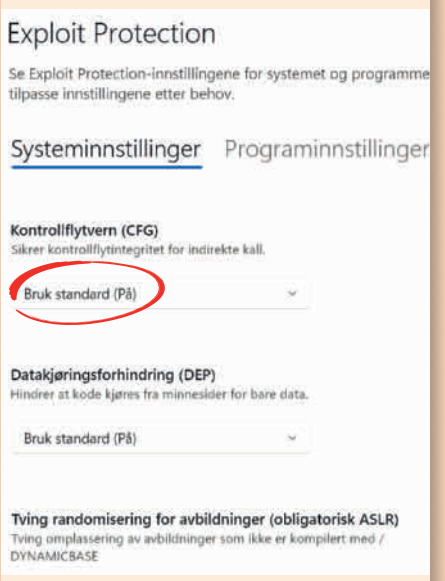


Det er lett å slå Bluetooth-tilkoblingen på og av fra Windows-innstillingene. Er den deaktivert, er du heller ikke synlig for andre enheter.

13

Beskytt pc-en mot farlig utnyttelse

Windows 10 og 11 er utrustet med robuste sikkerhetsfunksjoner som bidrar til å holde maskinen trygg. En av disse bærer det kryptiske navnet **Kontrollflytvern** og beskytter mot at skadelig kode kan utnytte sårbarheter på maskinen.



Pass på at denne beskyttelsen er aktivert i Windows-innstillingene under **Kontrollflytvern**.

14

Hold Windows oppdatert

Det passer nesten aldri når Windows ber deg om å fullføre en oppdatering ved å starte maskinen på nytt. Vi anbefaler likevel at du takker ja så snart som mulig når operativsystemet ber deg installere en oppdatering. Det skyldes at Microsoft sender ut viktige sikkerhetsoppdateringer til maskinen etter hvert som sårbarheter oppdages, slik at sikkerhetshullene kan elimineres.

15

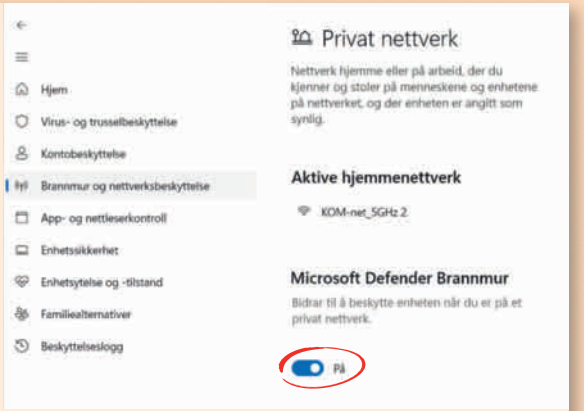
Husk regelmessig sikkerhetskopiering

Selv om de fleste ulykker kan unngås ved å følge de 100 tipsene på disse sidene, kan du rammes av skadevare eller løsepengevirus som ødelegger eller krypterer filer. Hvis det skjer, finnes det bare én sikker metode for å redde filene: Du må ha tatt en sikkerhetskopi slik at de kan gjenopprettes – for eksempel med Hasleo Backup Suite fra **komputer.no/2513**

16

Aktivering av brannmur

En brannmur er en viktig del av sikkerheten i Windows. Alle programmer og funksjoner som bruker nettverket eller internett, må først passere brannmuren i Windows, og det øker sikkerheten. Sjekk derfor i innstillingene at du har en aktiv brannmur på maskinen.



I Windows-innstillingene finner du kategorien **Brannmur og nettverksbeskyttelse**. Der ser du om brannmuren er aktivert og virker som den skal.

17

Bytt til en lokal konto

Hvis du er bekymret for utvekslingen av informasjon om bruken av pc-en på tvers av servere på internett, kan du benytte en lokal brukerkonto i Windows i stedet for en Microsoft-konto. Med en Microsoft-konto utveksles informasjon mellom maskinen og Microsofts servere, slik at du for eksempel kan synkronisere innstillinger mellom flere maskiner. Slik får du en lokal konto: **komputer.no/2513**

18

Grønne haker i sikkerhetsinnstillingene viser at alt er som det skal, og at antivirusprogrammet er aktivert.

Er antivirus aktivert?

Antivirusprogrammet er maskinens viktigste sikkerhetsprogram og holder konstant øye med alle filer du laster ned fra internett og alle programmer du starter på maskinen. Derfor er det avgjørende at programmet holdes oppdatert med de nyeste virusdefinisjonene, og at det til enhver tid er aktivt i bakgrunnen og beskytter maskinen.

Det kan du sjekke ved å åpne **Windows Sikkerhet** fra innstillingene i Windows. Deretter klikker du på feltet **Virus- og trusselbeskyttelse**.

19

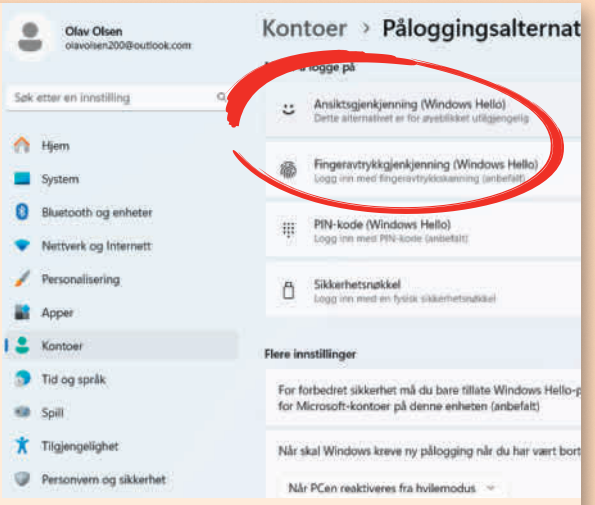
Unngå utdaterte programmer

Det virker kanskje ikke særlig viktig å ha den aller nyeste versjonen av et program, men det er det. Det faktisk avgjørende for å holde maskinen trygg. Hackere er flinke til å finne nye sikkerhetshull i kjente programmer. Det unngår du ved å holde programmene oppdatert med produsentens sikkerhetsoppdateringer.

20

Logg på med ansikt eller finger

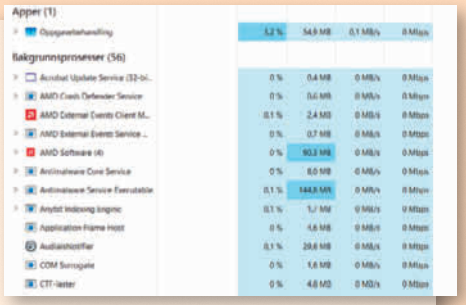
I Windows er det mulig å logge på med fingeravtrykk eller ansiktsgjenkjenning ved hjelp av funksjonen **Windows Hello**. Biometri er mye vanskeligere å forfalske enn det er å gjette et passord.



I innstillingene for **Kontoer** og **Påloggingsalternativer** kan du velge ansiktsgjenkjenning og fingeravtrykk.

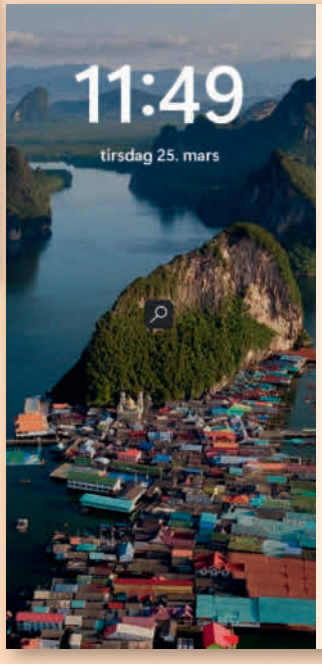
21

Sjekk hva som kjører i bakgrunnen



Oppgavebehandling åpnes ved at du trykker samtidig på tastene **Ctrl + Skift + Esc**.

Når et program eller en tjeneste kjører på maskinen, vises det i **Oppgavebehandling**. Der kan du også få oversikt over alle programmene som er aktive i bakgrunnen, og som ikke har et ikon liggende på oppgavelinjen. Selv om de fleste bakgrunnstjenester stammer fra Windows selv og har navn som ikke nødvendigvis er særlig forklarende, er det lurt å sjekke oversikten fra tid til annen. Ser du mistenkelige navn, bør du skanne maskinen for virus og skadevare.



22

Lås pc-en når du forlater den

Hvis maskinen aldri forlater hjemmet, er det neppe noen større risiko for at fremmede setter seg ved den og snoker i filene dine. Er den derimot med på reiser eller for eksempel en kafé, bør du alltid låse den når du går fra den – om det er for aldri så kort tid.

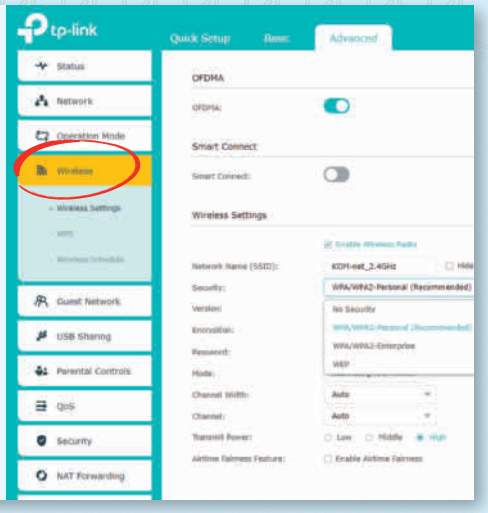
I Windows er det bare å trykke på **Windows-tast + L** for å bytte til låseskjermen.

23

Velg alltid den beste krypteringen

I ruterinnstillingene kan du velge mellom forskjellig kryptering av det trådløse signalet. Vi anbefaler de nyeste standardene: WPA2 eller WPA3. Sjekk veiledningen for ruteren for å se hvordan du kommer til og endrer innstillingene.

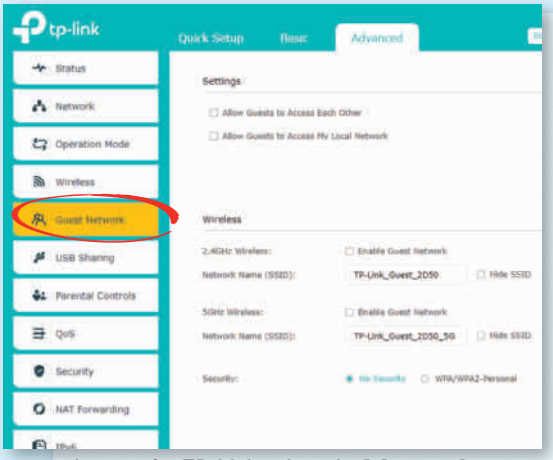
I rutere fra TP-Link velger du **Advanced** og deretter **Wireless**.



24

Lukk portene i ruteren

Forskjellige porter i ruteren gjør at du kan få tilgang til enheter og utstyr i hjemmet også når du er et annet sted. Har du ikke behov for dette, bør du lukke portene. I veiledningen for ruteren ser du hvordan du logger inn og finner oversikten over åpne porter.



I rutere fra TP-Link velger du **Advanced** og deretter **Guest Network**.

25

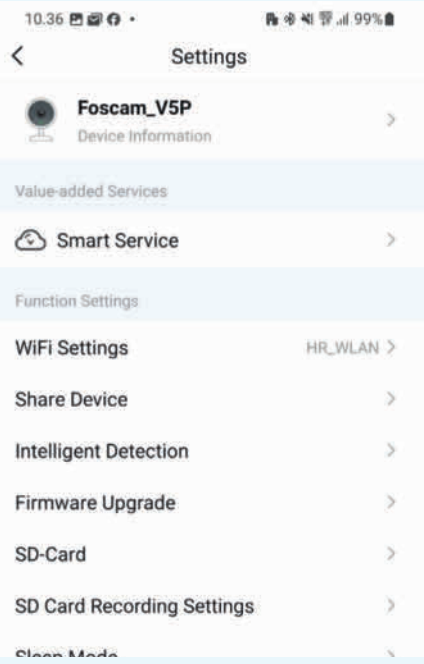
Lag et eget gjestenettverk

De fleste nyere rutere gjør det mulig å opprette et ekstra trådløst nettverk for besøkende. Dette nettverket gir ikke tilgang til andre enheter på det primære nettverket. Derfor er det en god løsning når man vil dele tilkoblingen. Nøyaktig hvordan gjestenettverket opprettes, kan du lese om i veiledningen for den aktuelle ruteren.

26

Hold smarte enheter oppdatert

Smarte enheter som stikkontakter og kameraer kan utgjøre en sikkerhetsrisiko for alle enheter på nettverket. Det kan du unngå ved å sørge for å holde slikt utstyr oppdatert med fastvareoppdateringer. Det gjør du direkte fra appene for de respektive enhetene.

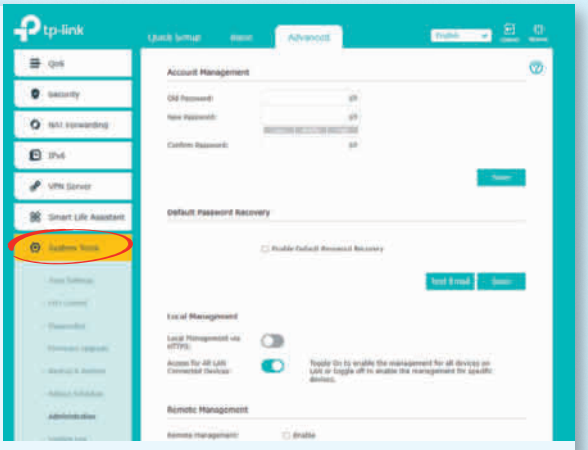


I appen for forskjellige smartenheter finner du også **Firmware Upgrade**, der det kan oppdateres.

27

Deaktiver fjernstyring av ruteren

Har du noen gang hatt behov for å få tilgang til ruteren når du ikke er hjemme? Hvis ikke, er det heller ingen grunn til at funksjonen skal være aktiv. Sjekk veiledningen for å finne ut hvordan du slår den av.

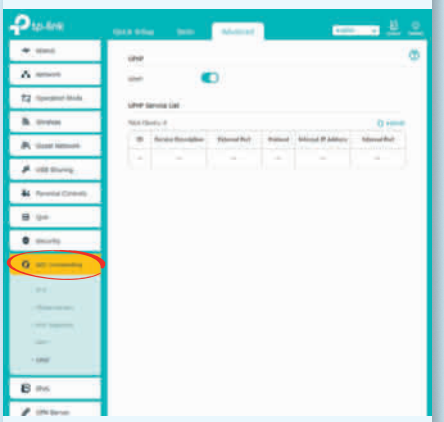


I rutere fra TP-Link må du gå via **Advanced** og **System Tools** for å deaktivere fjerntilgang.

28

Deaktiver UPnP i ruteren

Ruterfunksjonen UPnP, som du kan lese mer om på adressen komputer.no/2513, ble egentlig utviklet for å gjøre det lettere å koble sammen forskjellige typer utstyr på hjemmenettverket. I praksis har det vist seg at funksjonen også gjorde det betydelig enklere for uvedkommende å få tilgang til nettverket. Derfor anbefaler vi at du finner frem til funksjonen via brukerveiledningen til ruteren, slik at du kan logge inn og deaktivere UPnP.



Funksjonen UPnP finner du ofte i routerens avanserte meny under punktet **NAT Forwarding**.

29

Velg et langt og godt Wi-Fi-passord

Bruker du enkle ord eller tallrekker som passord til det trådløse nettet, inviterer du så å si uvedkommende til å koble seg til. Det samme gjelder hvis du ikke har giddet å endre produsentens standardpassord som fulgte med ruteren. I så fall bør du finne frem veiledningen og sjekke hvordan du endrer passord på det trådløse nettet.

30

Hold ruteren oppdatert

Det er viktig at du holder alt utstyr oppdatert. Det gjelder pc, mobil og smartenheter. Det samme gjelder for ruteren, som fortløpende mottar sikkerhetsoppdateringer fra produsenten. Derfor bør du gjøre det til en vane å se etter oppdateringer i ruterinnstillingene med jevne mellomrom. Det gjøres normalt fra menyen System.

31

Slå av ruterens WPS-funksjon

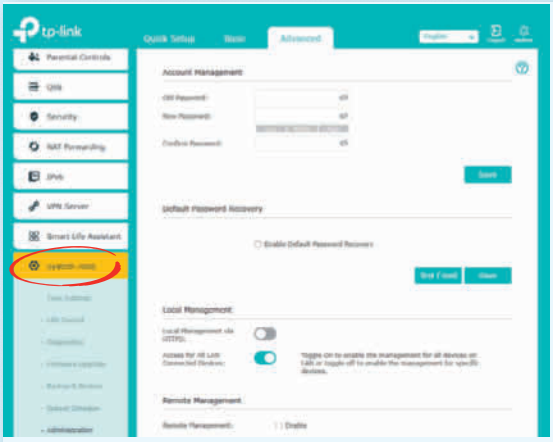
WPS finnes på både ruteren og de trådløse enhetene som kan kobles til nettverket. WPS gjør det mulig å koble til utstyr ved å trykke på en knapp, men kan også misbrukes. Derfor bør den slås av.

Bruker du ikke WPS, bør du deaktivere funksjonen fra ruterinnstillingene.

32

Ikke la det trådløse nettet være på til enhver tid

Hvis du har naboer, vil dere kunne se hverandres trådløse nettverk. Selv om et ubudent besøk på nettverket forutsetter at noen har fått tak i passordet ditt, kan du redusere risikoen betydelig ved å slå av ruteren om natten.



Du må som regel inn i menyen **System** i ruteren for å endre standard påloggingspassord.

33

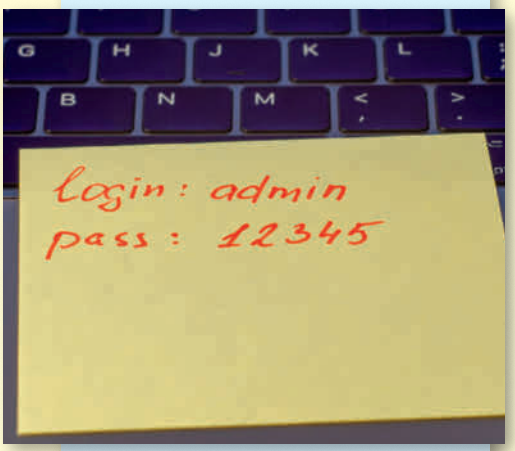
Endre passordet til den trådløse ruteren

Du må oppgi et passord og gjerne et brukernavn før du kan endre ruterinnstillingene. Derfor er det viktig at du har valgt passordet selv. Følg de oppdaterte rådene om sikre passord, og endre passordet fra ruterens egne innstillinger.

34

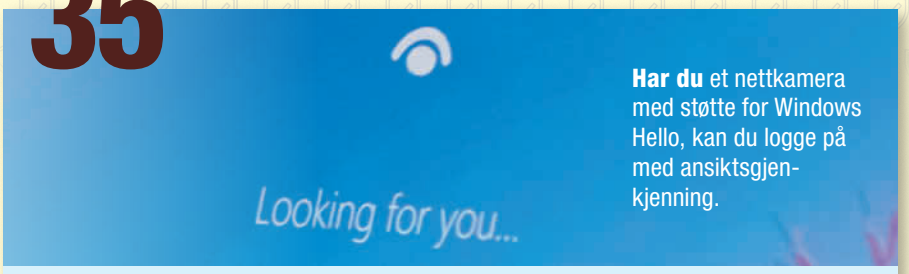
Unngå altfor opplagte passord

Det er fristende å velge passord som er lette å huske, særlig fordi vi lever i en tid der vi bruker passord til svært mange tjenester. Men fordi det alltid vil finnes mennesker med lav moral som forsøker å få tilgang til andres konto, er det viktig å ikke gjøre passordet for lett å gjette verken for mennesker eller avanserte programmer. Derfor gjelder det å unngå passord med logiske tallrekker eller vanlige ord. Les mer på: **komputer.no/2513**



De mest opplagte passordene er altfor lette å gjette. Derfor gjelder det å unngå tallrekker og ord du finner i en vanlig ordbok.

35



Har du et nettkamera med støtte for Windows Hello, kan du logge på med ansiktsgjenkjenning.

Logg på med ansiktsgjenkjenning eller fingeravtrykk

Du kan redusere antall vanskelige passord som må huskes, ved å erstatte dem med biometri der det er mulig. I Windows og på mobilen kan du velge ansiktsgjenkjenning eller fingeravtrykk som alternativ til det tradisjonelle passordet. Det er både enklere og mye sikrere.

36

Gjør passordene ekstra lange

Jo lengre et passord er, desto mer tid vil det ta for et program å bryte det eller et menneske å gjette det. Derfor anbefaler de fleste sikkerhetseksperter nå at passordene er på minst tolv tegn, og flere er enda bedre.

37

Regler og rim

Du kan gjøre det lange og sikre passordet lettere å huske hvis du forbinder det med noe som er viktig for deg. Det kunne for eksempel være et rim eller en sang som kombineres med tegn, tall og store bokstaver av typen dEtvar1gang-imaane$kinn!

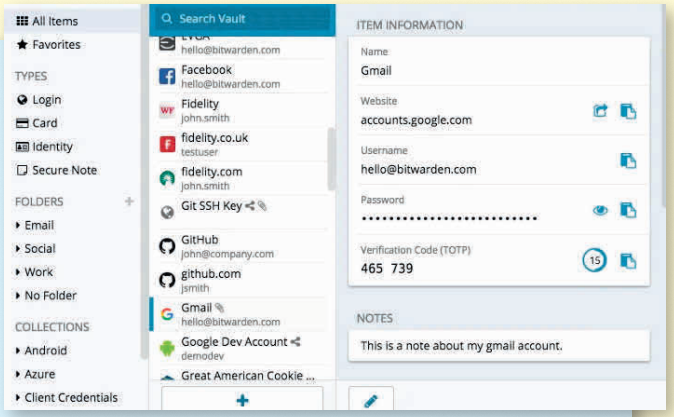
38

Bruk aldri samme passord flere steder

Det reduserer riktignok antallet passord du må huske, men du bør aldri bruke det samme passordet på flere nettsider og -tjenester. Gjør du det, kan i verste fall en hacker få fri tilgang til alle tjenestene, så lenge vedkommende har passordet til én av dem.

39

Bruk et passordprogram



Bitwarden Free er et glimrende passordprogram som holder orden på alle de sikre passordene.

Hvis du allerede synes at det kan være vanskelig å huske hverdagens mange passord, blir det bare verre etter hvert som passordene skal gjøres lengre og mer kompliserte. Det problemet kan du løse ved å benytte en passordgenerator. Det er et smart program som åpnes ved hjelp av et hovedpassord. Deretter sørger programmet for å holde orden på de kompliserte passordene til hver enkelt tjeneste og nettside. Du kan for eksempel bruke programmet Bitwarden Free, som du finner i sikkerhetspakken vår på **komputer.no/2513**.

40

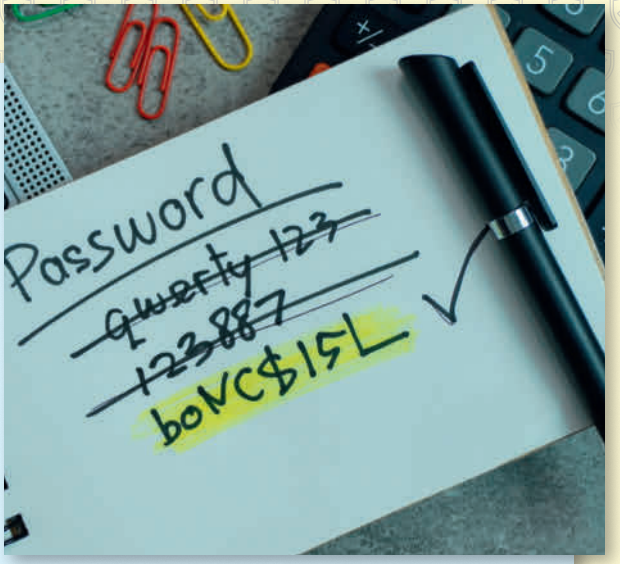
Er passordene lekket på nettet?

Fra tid til annen skjer det store datalekkasjer der hackere får tilgang til informasjon om brukerne av forskjellige tjenester. Ofte får de også tilgang til e-postadresser og passord, og det er naturligvis forbundet med en viss risiko hvis du benytter samme pålogging på flere tjenester. I Chrome kan du selv sjekke om passordene dine er lekket ved å gå til **Innstillinger**, velge **Personvern og sikkerhet** og **Sikkerhetssjekk**.

41

Et godt sammensatt passord

Oppskriften på et godt og robust passord har minst fire sikre ingredienser: Det skal bestå av både små og store bokstaver – gjerne tilfeldig spredt i passordet. Du bør også inkludere spesialtegn som @, !, % og lignende, som ikke er lette å gjette, i tillegg til tilfeldige tall. Les mer: komputer.no/2513



Dropp de logiske tall- og bokstavrekkene og lag i stedet et passord som umiddelbart virker tilfeldig.

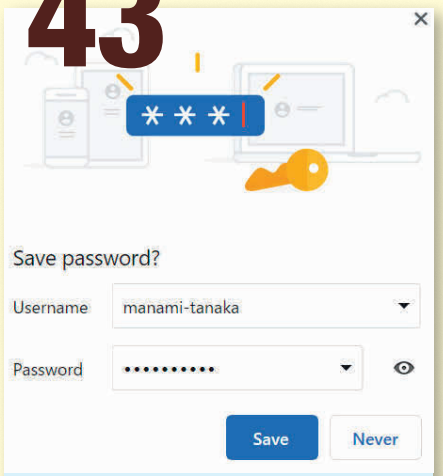
Med totrinnsautentisering benytter du også en tilfeldig engangskode.

42

Totrinnsautentisering har kommet for å bli

Det er en grunn til at BankID krever både personlig pålogging og en fysisk enhet i form av mobil eller nettbrett med en app der du bekrefter påloggingen. Det er kort sagt mye sikrere enn en løsning som kun består av et passord. Du kan få den samme høye sikkerheten for e-post ved å aktivere totrinnsautentisering i tjenesten.

43



Favorittnettleseren foreslår gjerne å lagre passord til hjemmesider for deg, men det er ikke uten en viss risiko.

Nettleseren bør ikke lagre passord

Det er fristende å takke ja når nettlesere som Edge og Chrome foreslår å lagre passordet til en hjemmeside for deg, men det er mindre sikkert enn et eget passordprogram. Det skyldes at passordene som regel er tilgjengelige og synlige for enhver som bruker pc-en, og at de ikke er spesielt godt beskyttet mot hackerangrep.

44

Navnet til hunden er ikke godt nok

Du tenker kanskje at fremmede aldri vil kunne gjette passordet når du har valgt navnet til et kjæledyr eller et barnebarn? Når det fraråddes av sikkerhetseksperter, skyldes det også at navn og ordentlige ord kan "gjettes" ved at spesialprogrammer gjør oppslag i ordbøker.

Navn på kjæledyr bør være strengt forbudt i passordene dine. Slike passord er altfor lette å gjette.

45

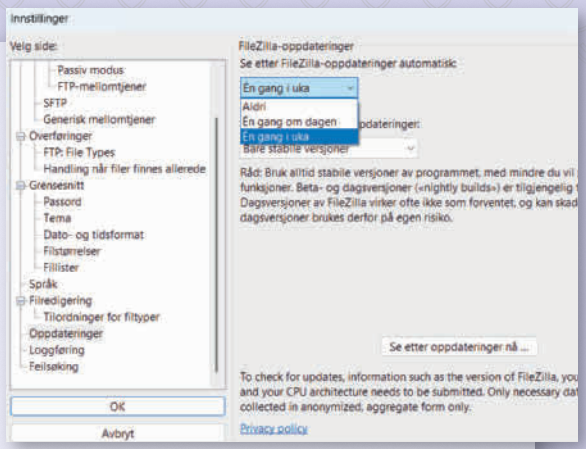
Unngå falske nedlastingssider

Det er ikke ufarlig å bruke en søkemotor som Google til å finne og laste ned et program på nettet. Du risikerer nemlig å havne på en falsk nedlastingsside der du kanskje tror at du laster ned et godt og legitimt program, men ender med en virusinfisert pc. Derfor bør du kun laste ned programmer direkte fra produsenten eller fra **komputer.no**, der alt er grundig sjekket for virus.

46

La programmene oppdatere seg selv

Programmer som ikke oppdateres på flere år, er notorisk usikre fordi hackere dermed har hatt god tid til å avdekke sikkerhetshull. Det unngår du ved å sørge for at programmene alltid er oppdatert. I de fleste programmer kan du velge å la dem søke etter og installere oppdateringer automatisk.



I de fleste programmer er det mulig å aktivere automatisk oppdatering. Du kan for eksempel få programmet til å sjekke en gang i uken.

Her er vi i ferd med å installere programmet doubleTwist, da Delta Toolbar plutselig dukker opp.

47

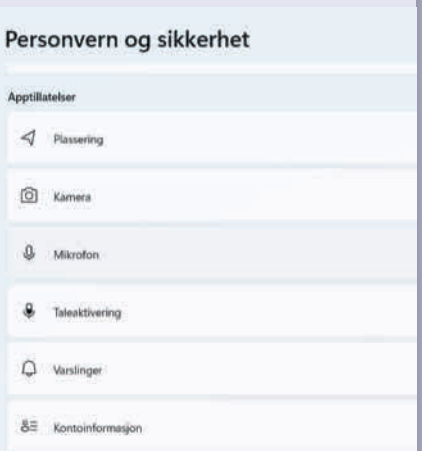
Unngå ekstratilbud under installering

Du må være særdeles våken når du installerer programmer på pc-en. Særlig gratisprogrammene har en lei tendens til å legge til valgfrie programmer, fordi det gir produsenten ekstrainntekt. Derfor bør du lese nøye hva du godtar under installeringen og takke nei til programmer du ikke kjenner.

48

Sjekk hvilke rettigheter du gir programmene

Er det ok at et program fra en mindre produsent får tilgang til posisjonsdata eller nettkameraet? Hvis ikke kan du gjennomgå programmets tillatelser: Høyreklikk på startknappen i Windows, og klikk på **Innstillinger**. Klikk på **Personvern og sikkerhet**, velg en tillatelse – som **Plassering** – og se hvilke programmer som har tilgang til informasjonen.



I Innstillingene under **Personvern og sikkerhet** ser du tillatelsene for alle de installerte programmene.

49

Avinstaller programmer du ikke bruker

Har du hatt maskinen i lengre tid, har du sannsynligvis også installert mange programmer i årenes løp – også programmer du ikke bruker lenger. Disse programmene kan utgjøre en sikkerhetsrisiko, og derfor bør du gjennomgå **Innstillingene** og avinstallere de du ikke bruker. Les mer her: **komputer.no/2513**

50

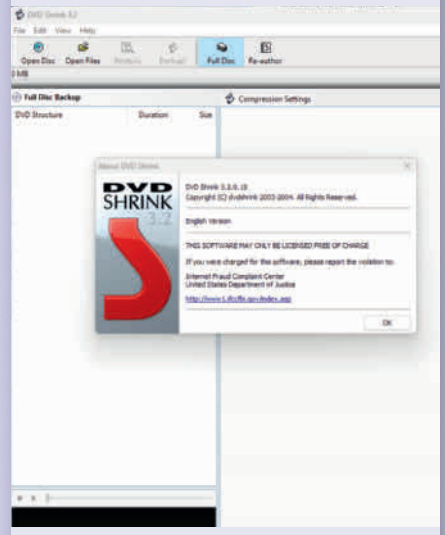
Er det løsepengevirus på maskinen?

Hvis pc-en virker tregere enn normalt, kan årsaken være skadevare som arbeider i det skjulte. De fryktede løsepengevirusene belaster for eksempel harddisken når de krypterer filer, slik at du kan presses for penger. Du kan sjekke diskaktiviteten i Oppgavebehandling ved å trykke på **Ctrl + Skift + Esc** og åpne fanen **Disk**.

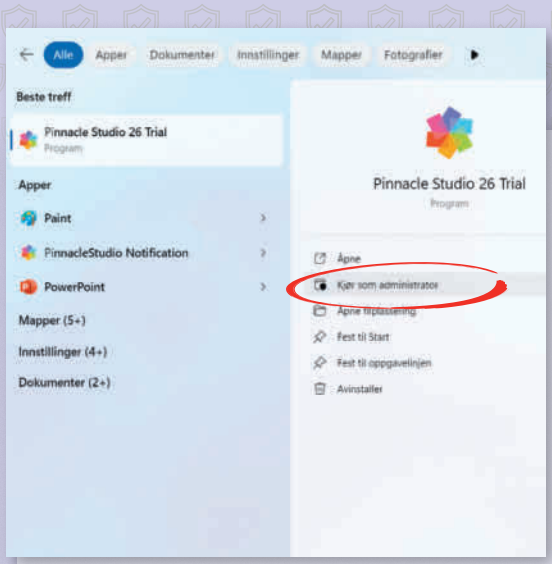
51

Blir programmet fortsatt oppdatert?

Selv gode programmer mister til tider produsentens støtte, og da blir det ikke lenger oppdatert. Da får du heller ikke tettet sikkerhetshull, og dermed blir det risikabelt å fortsette å bruke det utdaterte programmet. Derfor bør du med jevne mellomrom sjekke når programmene sist ble oppdatert.



DVD Shrink er et godt program til å lagre dvd-film på harddisken, men den siste oppdateringen kom i 2004, og derfor er det ikke lenger trygt å bruke.



Søkeresultatene i startmenyen gjør det mulig å kjøre programmer som administrator.

52

Gi ikke uhindret tilgang til pc-en

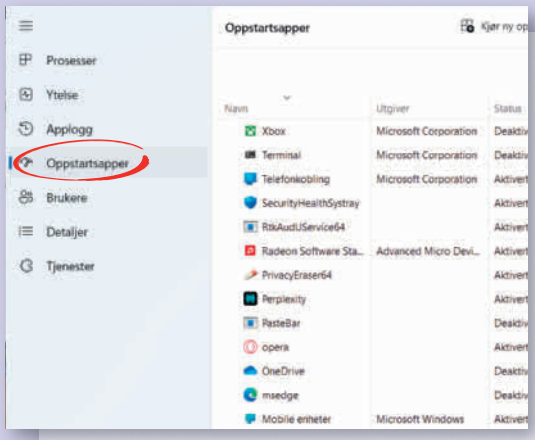
Når du søker etter programmer i startmenyen eller høyreklikker på en snarvei, kan du velge å kjøre programmet som administrator. Det bør du aldri gjøre, med mindre det må til for at programmet skal fungere. Administratortilgang gir nemlig programmene langt flere tillatelser på maskinen.

53

Sjekk heller filene en gang ekstra

Du kan ikke alltid stole fullt og helt på antivirusprogrammet når det frikjenner et program eller en fil. Vil du være helt sikker, må du sjekke med en uhildet tredjepart. Vi anbefaler nettsiden **virustotal.com**. Der kan du laste opp filer og få svar på hvordan de vurderes av alle ledende sikkerhetsprogrammer som finnes på markedet.

På VirusTotal klikker du på **Choose file** og velger en fil på harddisken. Da får du straks vite om filen er farlig.



Oppstartsapper i Oppgavebehandling viser apper som starter sammen med Windows.

54

Begrens antall oppstartsprogrammer

De små programmene som starter automatisk sammen med Windows, legger ikke bare beslag på maskinens ressurser. Det kan også finnes ondsinnede programmer blant dem. Ta derfor en kritisk gjennomgang av fanen **Oppstartsapper** i Oppgavebehandling, som du åpner med **Ctrl + Skift + Esc**.

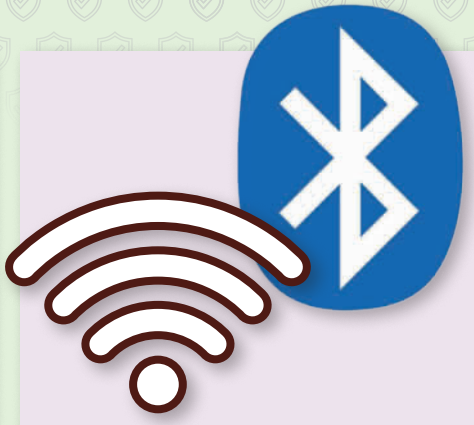
55

Gi programmene begrenset tilgang

Løsepengevirus er en virustype som først krypterer filene dine, før det krever at du betaler løsepenger for å få låst dem opp igjen. Hvis ikke viruset har tilgang til filene, kan det heller ikke kryptere dem. Lås derfor mappene med **Kontrollert mappetilgang** i Windows-innstillingene.

56
Installer antivirus

Du som bruker iPhone er allerede godt beskyttet. Har du derimot en Android-mobil, er det særdeles fornuftig å beskytte seg med et antivirusprogram – akkurat som på pc-en. Sophos Intercept X for Mobile er den beste gratis antivirus-appen for Android, og på nettsiden vår forklarer vi hvordan du bruker den. Artikkelen finner du her: komputer.no/2513



Det er ingen grunn til at verken Wi-Fi eller Bluetooth skal være aktivert når du ikke bruker de trådløse tilkoblingene.

57
Slå av Bluetooth og Wi-Fi

Wi-Fi og Bluetooth er smarte trådløse forbindelser, men for hackere kan de kan også være en vei inn på mobilen. Du bør kun ha aktivert Wi-Fi når du er på trådløse nettverk som er til å stole på. Bluetooth bør bare være aktivert når du bruker et trådløst hodesett eller ditto høyttalere. Ellers er det lett å slå av disse tilkoblingene midlertidig fra innstillingene på mobilen.

58
Hold mobilen oppdatert

Det kan oppstå sikkerhetshull og sårbarheter i programvaren til mobilen, og det kan hackere utnytte. Derfor bør du forsikre deg om at operativsystemet er oppdatert. Du sjekker om det finnes en oppdatering ved å åpne innstillingene på en iPhone eller Android-mobil og gå til kategorien for programvareoppdateringer eller informasjon om enheten.

I innstillingene på mobilen er det lett å se om alt er oppdatert.

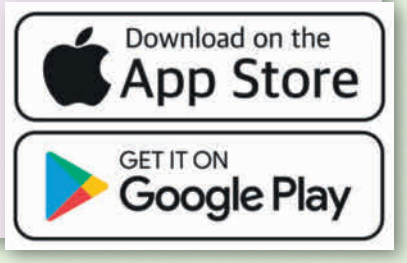
59
Et godt passord for delt internett

Det er nyttig at det er mulig å dele mobildata og logge på internett fra en annen enhet via mobilens nett-tilkobling. Gjør du det, er det viktig at du beskytter tilgangen med et robust passord. Passordet endrer du fra mobilens innstillinger, der du også aktiverer Delt internett. Husk å bruke både små og store bokstaver samt spesialtegn og tall i passordet.

60
Hold deg til de offisielle appbutikkene

For en hacker er det lettest å ta seg inn på mobilen via en app. Noen apper er fulle av skadevare som kan føre til at du får tømt bankkontoen eller blir overvåket. Derfor bør du holde deg til de offisielle appbutikkene.

På iPhone laster du ned apper fra App Store. I Android velger du Play Butikk.



61

Er ikke appene oppdatert, blir det lettere for hackere å infisere dem med skadevare.

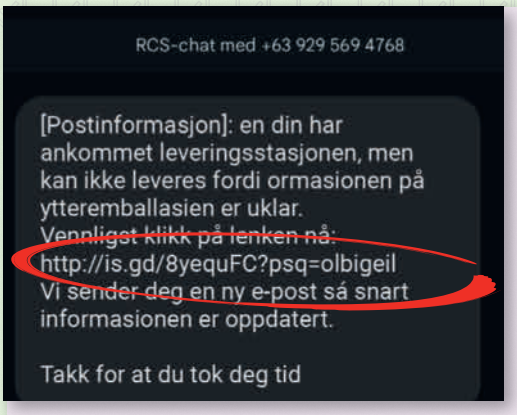
Hold alle apper oppdatert

På samme måte som at det er viktig å holde operativsystemet på mobilen oppdatert, må du også huske å oppdatere appene med jevne mellomrom. Da kan du bruke appene med ro i sinnet. Les om hvordan du oppdaterer apper på komputer.no/oppdater-apper

62

Husk sikkerhetskopier av alle bilder

For de fleste er mobilen også et kamera som er med overalt, og derfor lagrer de fleste bildene lokalt på mobilen. Skjer det noe med mobilen, risikerer du altså å miste bildene, med mindre du også har lagret dem et annet sted. De bør altså sikkerhetskopieres. Hvordan det gjøres, ser du her: **komputer.no/2513**



Svindelmeldingen er gjerne utstyrt med en kobling som du oppfordres til å trykke på.

63

Vær på vakt mot sms-svindel

Som med e-post vil du også oppleve svindelforsøk via tekstmeldinger. Det kan for eksempel være en tekstmelding om en pakke som ikke ble levert – som i skjermbildet til venstre. Det kan også være falske meldinger fra myndighetene eller varsel om at du har vunnet en premie.

64

Unngå offentlige USB-kontakter

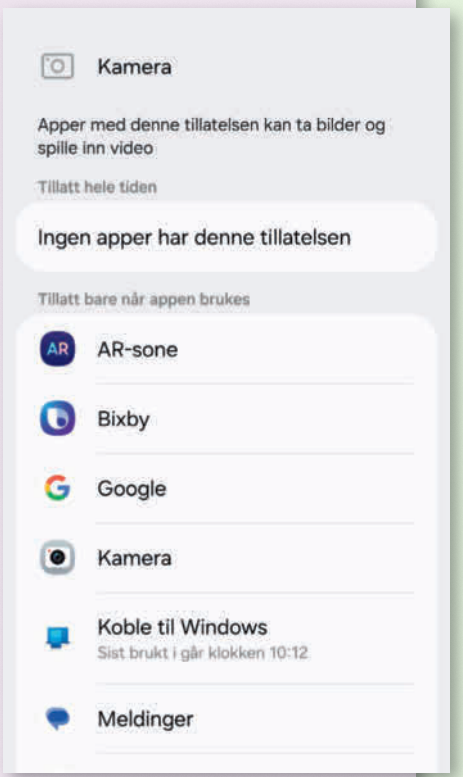
Det kan være fristende å benytte anledningen til å lade via offentlig tilgjengelige USB-ladere, men vær på vakt! Hackere bruker ofte slike uttak til å installere skadevare på mobilen. Metoden kalles ”juice jacking”, og også her er hensikten å stjele personopplysninger.

65

Sjekk apptillatelsene

Du bør gjennomgå hvilke apper som har tilgang til de ulike verktøyene på mobilen. På en Samsung-mobil finner du oversikten over tillatelser under **Innstillinger** og kategorien **Apper**, og **Apptillatelser.** Metoden kan være litt annerledes hvis du har en mobil av et annet merke, men du må som regel inn i appinnstillingene for å finne oversikten over tillatelser, der du lett kan deaktivere uønskede tillatelser.

Du bør være særlig kritisk til hvilke apper som skal ha tilgang til mikrofon, GPS, kamera, anrop og meldinger.



Ingen apper bør ha permanent tilgang til for eksempel mobilkameraet. Hvis det er tilfellet, bør du fjerne tillatelsen.

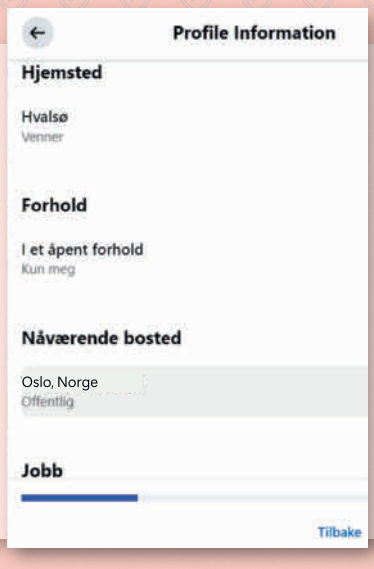
66

Lås mobilen med biometri

Biometri, som fingeravtrykk eller ansiktsgjenkjenning, gjør det mulig å låse opp mobilen raskt og uten passord. Det er også en sikker metode for å beskytte data, fordi du må være fysisk til stede med ansikt eller fingeravtrykk for å kunne låse opp mobilen.

Det er mulig å aktivere biometriske funksjoner i sikkerhetsinnstillingene.

Foto: Marco Rosales, patpitchaya, Hakim Ullah ID 4268939, Inna Kharlamova, Yalcin Sonat/Shutterstock.com



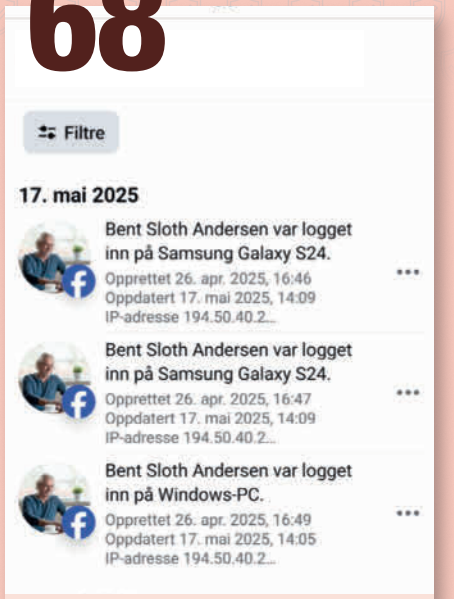
67

En privat profil

Du kan gjøre profilen din privat og redusere faren for identitetstyveri ved å klikke på profilbildet øverst til høyre i Facebook og deretter velge **Innstillinger og personverninnstillinger**. Velg **Kontroll av personverninnstillinger**, og gjennomgå kategoriene på siden.

Du bør sørge for at det kun er deg, familie og venner som kan se personlig informasjon om bosted, jobb og forhold på Facebook.

68



Ser du en enhet du ikke gjenkjenner, klikker du på de tre prikkene ved enheten og velger **Logg ut**.

Sjekk hvor du er pålogget

Mistenker du at andre har tilgang til profilen, kan du sjekke det ved å klikke på profilbildet øverst til høyre. Velg **Innstillinger og personvern**. Deretter klikker du på **Aktivitetslogg** fulgt av **Hvor du er innlogget**. Da ser du alle enheter du har vært innlogget med.

69

Falskt innhold

Facebook har droppet faktasjekken, og derfor finnes det mengder av uriktige fakta på plattformen. Slikt innhold er dessverre ikke bare løgnaktig. Det kan også være direkte farlig å klikke på det. En kobling til en falsk artikkel kan for eksempel ta deg til en svindelside der du blir lurt til å oppgi følsom informasjon, eller du risikerer å få virus på maskinen. Vær alltid kritisk til det du leser på Facebook.

70

Husk å logge av

Det virker kanskje opplagt, men du må huske å logge av Facebook når du ikke bruker tjenesten. Det gjelder spesielt hvis du har vært pålogget fra en offentlig maskin eller fra en pc du deler med andre. Hvis ikke risikerer du at uvedkommende får tilgang til profilen din.

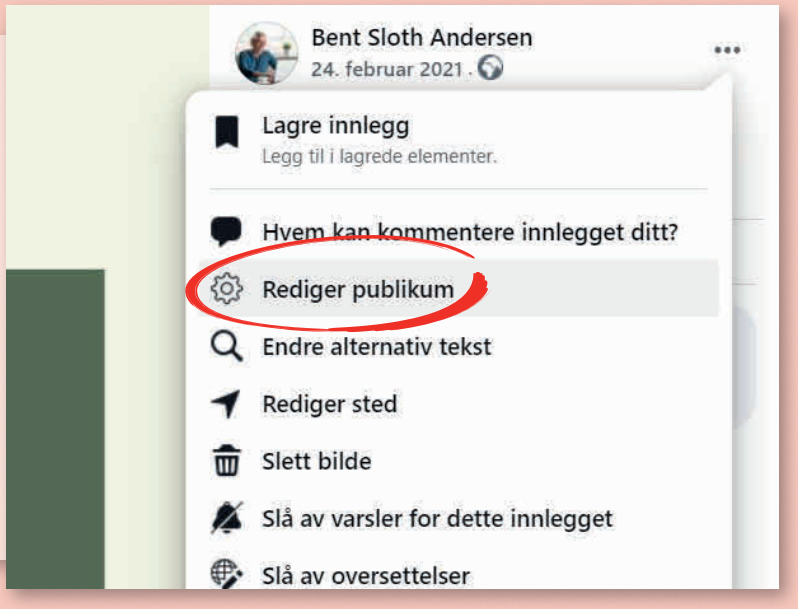
Etter avlogging må du sjekke at ikke nettleseren har lagret brukernavn og passord. I så fall må du passe på at det blir slettet.

71

Gjør profilbildet privat

Svindlere bruker gjerne Facebook til å rappe identiteten til tilfeldige ofre og bruke den til å lure andre. På mange Facebook-profiler er det nemlig fri tilgang til profilbilder som det er lett for uærlige sjeler å laste ned, lagre og misbruke. Det kan du hindre ved å gjøre profilbildet privat, slik at bare du og dine venner kan åpne bildet. Det er fortsatt mulig for andre å se bildet, men bare i et miniformat som er stort sett ubrukelig til alt annet.

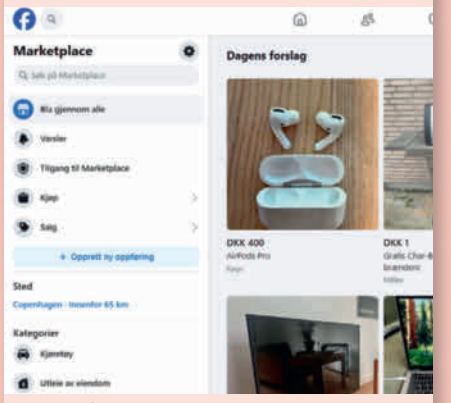
Åpne profilbildet og klikk på de tre prikkene. Klikk på **Rediger publikum**, og velg dine venner.



72
Vær forsiktig på markedsplassen

Facebook Marketplace er navnet på markedsplassen til Facebook, der du kan kjøpe og selge varer, men det er mange eksempler på at både kjøpere og selgere har blitt svindlet.

En selger vil for eksempel tilby merkevarer eller designerklær til urealistisk lave priser, men sender i virkeligheten en kopi eller ingenting. Et annet eksempel er kjøpere som vil betale via tvilsomme tjenester der du ikke kommer til å se snurten av pengene dine. Dessuten risikerer du å kjøpe tyvegods.



Du må være særlig aktsom når du handler på Facebook Marketplace.

73
Koblinger i Messenger

Får du en melding ut av det blå på Facebooks nettprattjeneste Messenger der du oppfordres til å klikke på en lenke, er det all mulig grunn til å være skeptisk. Det gjelder særlig hvis du får melding fra en fremmed, men du bør også være på vakt hvis det er en av dine egne Facebook-venner som står som avsender. Noen kan ha hacket profilen til vedkommende.

I så fall kan du ringe vedkommende for å få bekreftet eller avkreftet at meldingen er ekte.

74
Tenk gjennom hva du deler

Facebook er utviklet nettopp for å få deg til å dele opplevelser og tanker med familie og venner. Nettopp derfor bør du tenke over hva du egentlig deler.

Er ikke profilen din privat, kan i utgangspunktet hvem som helst se hva du deler og bruke informasjonen mot deg. Det gjelder ikke bare statusoppdateringer, men i høy grad også hva som står om deg i profilen. Du bør vurdere å skjule slik privat informasjon. Her ser du hvordan: **komputer.no/2513**

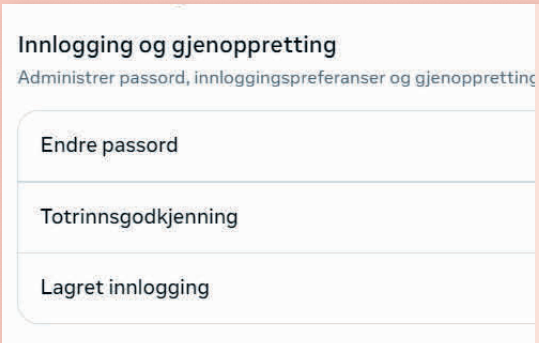
75
Aktivering av varsler

I Facebook-innstillingene kan du aktivere en funksjon som varsler hvis noen får tilgang til kontoen fra en uvanlig plassering. På den måten kan du reagere umiddelbart og logge vedkommende ut igjen. Deretter bør du øyeblikkelig endre passordet.

Funksjonen finner du i personverninnstillingene ved å klikke på **Kontroller varslene dine** og deretter **Slik beskytter du kontoen din**.

76
Ikke bli venn med noen du ikke vet hvem er

Du bør være forsiktig med å akseptere hvis noen du verken kjenner eller har truffet vil bli venn med deg på Facebook. Det gjelder særlig hvis dere ikke har felles venner. Da er det stor fare for at det er svindel. Her ser du hvordan du oppdager at en profil er falsk: **komputer.no/2513**



I innstillingene for beskyttelse av kontoen kan du både bytte passord og aktivere totrinnsgodkjenning.

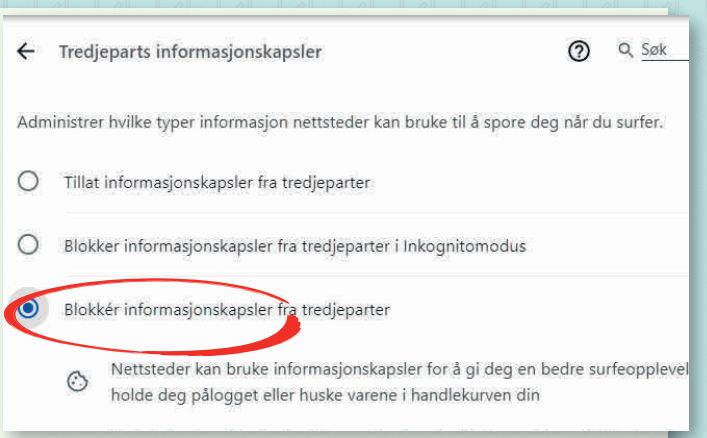
77
Bruk totrinnsgodkjenning

Totrinnsgodkjenning på Facebook krever at du oppgir en kode fra mobilen i tillegg til det vanlige passordet når du logger inn. Det gjør det vanskeligere for hackere å få tilgang til kontoen. Totrinnsgodkjenning aktiveres fra sikkerhetsinnstillingene.

78
Informasjonskapsler som sladrer

Informasjonskapsler (også kjent som cookies) kan lagre preferanser på nettsider du besøker ofte, slik at det går raskere å laste dem inn, men kapslene benyttes også til å spore deg på tvers av nettsider. Det gjelder særlig tredjepartskapsler. De stammer nemlig fra andre kilder enn den nettsiden du besøker.

Informasjonskapsler fra tredjeparter kommer gjerne fra reklameselskaper som sporer ferden din på nettet, for så å overlesse deg med annonser som er tilpasset det du foretar deg og interesserer deg for. Det betyr at annonsene du ser på ulike nettsider, vil henge sammen med hva du tidligere har foretatt deg på nettet. Det er ganske inngripende og er noe de fleste ønsker å unngå.



Du kan blokkere tredjepartskapslene i de fleste nettlesere. I Chrome finner du innstillingene under **Personvern og sikkerhet**.

I Chrome kan du sjekke tillatelser ved å åpne innstillingene for personvern og sikkerhet og velge **Nettstedsinnstillinger**. Der kan du gjennomgå tillatelsene og se hvilke nettsider som har fått tilgang til hva.

79
Gjennomgå tillatelser

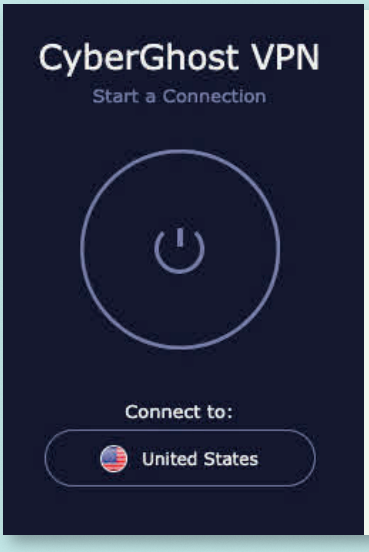
Mange hjemmesider ber om tilgang til maskinens komponenter, som kamera, mikrofon og stedsdata, mens andre sider vil ha lov til å sende deg varslinger i nettleseren. Gjør det gjerne til en vane å gjennomgå og tilpasse tillatelsene med jevne mellomrom, slik at du ikke gir hjemmesider unødvendig mange friheter.

80
Avslutt nettleseren med jevne mellomrom

Å ha nettleseren åpen i dagevis er både en belastning for maskinen og en potensiell sikkerhetsrisiko. Når du lukker nettleseren, slettes visse midlertidige filer og øktkapsler, som ellers kan utnyttes av hackere til å følge med på hva du foretar deg. Gjør det til en vane å lukke nettleseren daglig.

81
Fjern lagrede passord

Det kan virke praktisk å la nettleseren huske alle passord, men det utgjør en sikkerhetsrisiko. Hvis maskinen eller Google-kontoen (hvis du bruker Chrome som nettleser) blir kompromittert, er det lett for uvedkommende å få tilgang til alle påloggingsdata. På nettsiden vår viser vi hvordan du kan fjerne lagrede passord fra både Chrome og Edge:
komputer.no/2513



82
Bruk VPN

En VPN krypterer internettilkoblingen og skjuler maskinens IP-adresse. Det gjør det vanskeligere for nettsider og hackere å overvåke deg. De fleste VPN-tjenester må man betale for, men CyberGhost VPN Free Proxy er gratis. Her ser du hvordan du bruker utvidelsen: komputer.no/2513

Med nettleserutvidelsen CyberGhost VPN Free Proxy får du en god og gratis VPN til Chrome og Firefox, slik at du kan skjule IP-adressen.

83
Klikk aldri på annonser

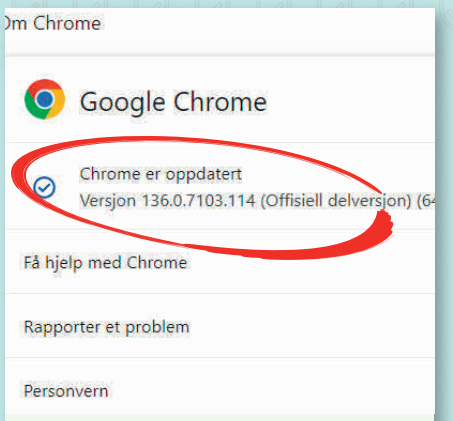
Annonser på nettsider er mer enn bare irriterende. Noen av dem er nemlig utviklet for å ta deg til useriøse nettsider eller installere skadevare på maskinen. Annonsene bruker falske advarsler eller tilbud på produkter eller pc-programmer til å få deg til å klikke på dem.

Selv tilsynelatende legitime annonser kan være falske. Derfor bør du unngå å klikke på annonser nær sagt uansett – med mindre du er helt sikker på hvem som står bak.

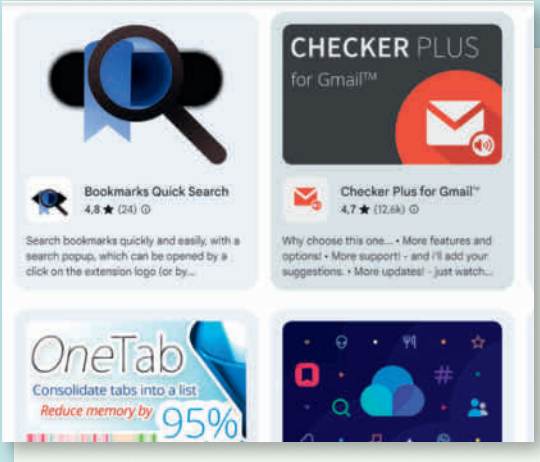
84
Forsiktig med hva du laster ned

Mange sikkerhetsproblemer starter med en lite gjennomtenkt nedlasting fra nettet. Unngå å laste ned filer fra ukjente eller lite troverdige kilder. Er du i tvil, bør du alltid skanne filer du laster ned, med antivirusprogrammet.

Vær særlig oppmerksom på nettsider som lokker med gratisversjoner av ellers dyre programmer. Husk at hvis noe virker for godt til å være sant, så er det som regel det.



Bruker du Chrome, kan du sjekke om nettleseren er oppdatert under **Om Chrome** i innstillingene.



Les anmeldelsene av utvidelser når du vil hente dem fra for eksempel Chrome Nettmarked.

86
Sjekk utvidelser grundig

Nettleserutvidelser kan gjøre mye godt, men de kan også være skadelige. Sjekk derfor hvilke utvidelser du har installert, og fjern de du ikke bruker. Sjekk også anmeldelser og utgiverens troverdighet. Her viser vi hvordan du fjerner utvidelser: komputer.no/2513

85
Hold nettleseren oppdatert

Gamle nettleserversjoner har, som så mye annen programvare, ofte sårbarheter og sikkerhetshull som hackere vet å utnytte.

Sikkerhetshullene tettes fortløpende etter hvert som nettleseren oppdateres, og de fleste, for eksempel Google Chrome og Microsoft Edge, oppdateres automatisk. Det krever likevel at du starter nettleseren på nytt ved å lukke den og åpne den igjen.

87
Velg en sikker nettleser

Noen nettlesere, som Firefox og Brave, har særlig fokus på personvern og sikkerhet og gir i utgangspunktet bedre kontroll over hva som deles med tredjeparter. Brave blokkerer automatisk sporingskapsler og annonser, mens Firefox har avanserte personverninnstillinger. Begge kan lastes ned her: komputer.no/2513

Brave og Firefox er gode valg for deg som legger vekt på personvernet.

88
Vær oppmerksom på domenesvindel

Nettfiske skjer ofte via domener som ligner kjente sider, men med små variasjoner, som ”faceboook.com” i stedet for ”facebook.com”. Sjekk domenet nøye før du logger inn eller laster ned noe som helst. I verste fall kan et enkelt besøk på feil side gi en hacker tilgang til privat informasjon.

89
Bruk Trustpilot og Forbrukerrådet

Etter at merkingen Trygg e-handel ble lagt ned i 2023, har vi ingen tilsvarende ordning i Norge. Det gjør det desto viktigere å sjekke brukererfaringer. Søk etter nettbutikken på **no.trustpilot.com** og les andres erfaringer, særlig hvis du ikke kjenner butikken fra før. Sjekk også siden til **forbrukerradet.no** om netthandel. Der får du også hjelp ved eventuelle tvister.

Trustpilot er en global tjeneste og har også en norsk side som gir en god pekepinn om hva en nettbutikk er god for.

90
Ikke bruk en offentlig pc

Offentlig tilgjengelige maskiner, som du finner på biblioteker, hoteller og så videre, kan være utsatt. Når du handler på nett, oppgir du følsom informasjon om betaling og adresser, og det bør ikke uvedkommende få tak i. Bruk alltid din egen pc når du handler på nett. Sørg for at den alltid er oppdatert og har et godt antivirusprogram.

91
Les vilkårene grundig

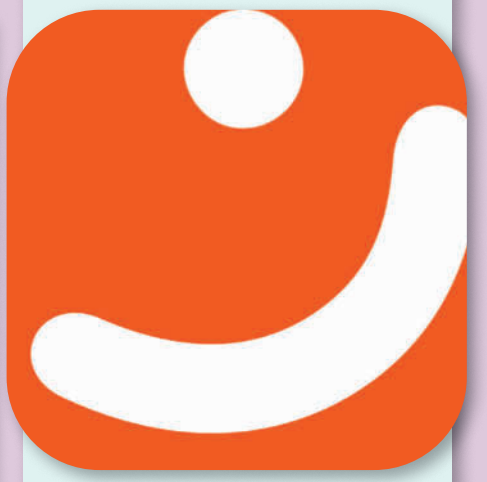
Mange klikker raskt på "godta" uten å lese kjøpsvilkårene, men de inneholder viktig informasjon som regler om returrett, leveringstider og gebyrer. Særlig ved kjøp fra utlandet kan det komme til ekstra omkostninger, og forbrukerbeskyttelsen kan være dårligere. Bruk litt tid på å lese vilkårene, slik at du vet hvilken avtale du inngår.

92
Sjekk butikkens fysiske adresse

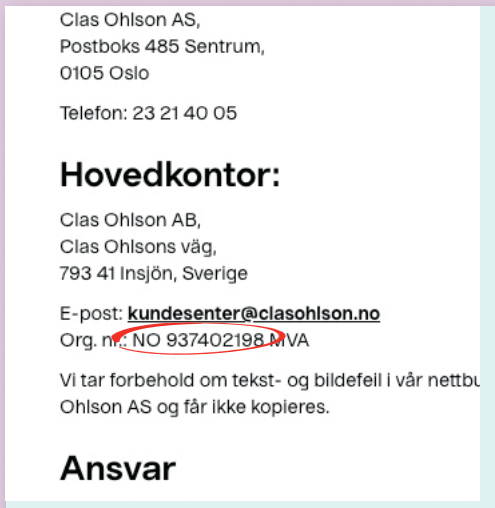
En seriøs nettbutikk oppgir alltid sin fysiske adresse. Det er et dårlig tegn hvis adressen mangler eller virker tvilsom. Bruk Google Maps til å sjekke om adressen eksisterer og matcher firmaprofilen. Mange svindelbutikker benytter fiktive adresser eller henviser til kontorhoteller. Det er generelt et tegn på at du bør velge noe annet.

93
Betal med Vipps

Vipps er en rask og sikker betalingsmetode når du handler på nettet. Velger du denne betalingsmetoden, deles ikke kortinformasjonen med nettbutikken. Fordi du godkjenner betalingen fra mobilen, har du også bedre kontroll med betalingene. Dessuten registreres transaksjonen tydelig i både appen og i banken, slik at dokumentasjonen er på plass hvis det skulle oppstå problemer. Derfor bør du velge Vipps der det er mulig.



Med Vipps får ikke butikken tilgang til kortnummeret. Dermed er du trygg også hvis nettbutikken blir hacket.


Clas Ohlson AS,
Postboks 485 Sentrum,
0105 Oslo

Telefon: 23 21 40 05

Hovedkontor:

Clas Ohlson AB,
Clas Ohlsons väg,
793 41 Insjön, Sverige

E-post: kundesenter@clasohlson.no
Org. nr.: NO 937402198 MVA

Vi tar forbehold om tekst- og bildefeil i vår nettbu
Ohlson AS og får ikke kopieres.

Ansvar

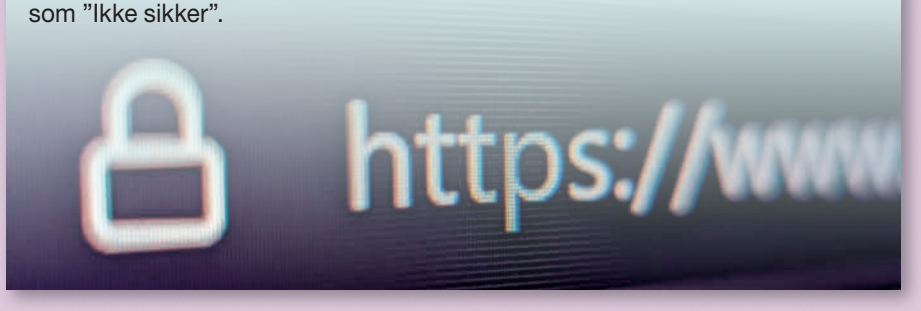
Organisasjonsnummeret står gjerne nederst eller øverst på nettsiden.

94
Sjekk butikkens organisasjonsnummer

En rask og enkel metode for å sjekke om du handler med et seriøst selskap er å sjekke organisasjonsnummeret, som du finner på butikkens hjemmeside. Organisasjonsnummeret viser selskapets offisielle registrering i Norge. Ved å søke opp nummeret på **brreg.no**, ser du om selskapet finnes og hvem som står bak. Manglende eller falskt organisasjonsnummer betyr at du bør holde deg unna.

95
Handle kun fra nettsider med https

Hvis det står ”https” og vises en hengelås i adresselinjen, betyr det at forbindelsen mellom maskinen din og nettbutikken er kryptert. Det beskytter informasjonen mot å bli snappet opp av tredjeparter. Hvis det kun står ”http”, bør du unngå å oppgi personlige data, og det gjelder spesielt betalingsinformasjon. I dag markerer de fleste nettlesere hjemmesider uten en sikker tilkobling som ”Ikke sikker”.



96
Det største norske bruktmarkedet

Det går nesten alltid bra å handle på finn.no, men svindel er en reell trussel også her. Derfor bør du aldri betale forskudd. Avtal helst et fysisk møte, og betal først når varen overleveres. Skal den sendes, anbefaler FINN at du bruker tjenesten Fiks Ferdig. Da tar de hånd om betaling og sending, slik at kjøper får varen og selger får pengene.

Velg selgere som har fått gode vurderinger og er verifisert med BankID.

97
Nettauksjoner

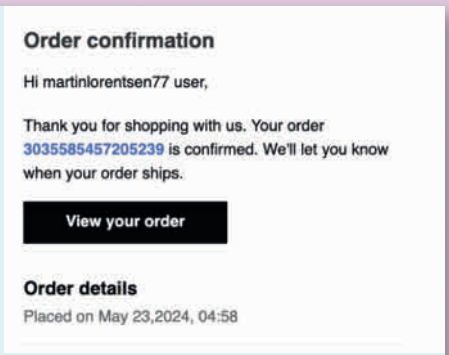
Ved kjøp fra en norsk nettauksjon, som qxl.no, gjelder forbrukerkjøpsloven kun når du kjøper fra næringsdrivende. Kjøper du fra privatpersoner er rettighetene svakere. Handler du på ebay, kan du ha angre- og reklamasjonsrett hvis butikken ligger i EU/EØS, men sjekk sluttsummen inkludert frakt og avgifter, og les andre brukeres erfaringer med selgeren.

98
Sjekk bankkontoen etter handelen

Når du har handlet på nett, er det en god vane å sjekke nettbanken. Pass på at beløpet du har godkjent, stemmer med det som er trukket. Uautoriserte eller doble trekk kan være tegn på feil eller misbruk. Oppdager du noe mistenkelig, bør du øyeblikkelig kontakte banken. Jo raskere du reagerer, desto bedre.

99
Lagre ordrebekreftelsen

Lagre alltid ordrebekreftelsen når du har handlet. Den kommer gjerne som e-post eller pdf og fungerer som dokumentasjon på hva du har kjøpt, når og til hvilken pris. Det er nyttig ved retur og reklamasjon, eller hvis varen aldri dukker opp. Husk å lagre ordrebekreftelsen et trygt sted, slik at du alltid kan finne den igjen.


Order confirmation

Hi martinlorentsen77 user,

Thank you for shopping with us. Your order 303558545720523 9 is confirmed. We'll let you know when your order ships.

View your order

Order details

Placed on May 23,2024, 04:58

En ordrebekreftelse dokumenterer hva du har kjøpt og hva varen kostet – hvis det skulle oppstå uenighet om sluttsummen.

100
Sjekk avsenderland

Det er ikke alltid like opplagt hvor en vare sendes fra når du handler på nettet. Nettbutikker kan ha norsk navn og domene, men sender varene fra Kina eller andre land utenfor EU/EØS. Det kan gi lang leveringstid, høyere fraktkostnad og tillegg i form av toll og moms. Sjekk alltid leveringsinformasjon i vilkårene før du bestiller. Det står med liten skrift, men kan ha stor betydning for sluttsummen.

Det kan koste dyrt hvis varen du kjøper på nettet, kommer langveis fra.

Foto: Ryan DeBerardinis, nik_nadal/Shutterstock.com