100 effektive tips til din sikkerhed

Din digitale færden på internettet, mobilen og computeren er fyldt med ukendte faldgruber. Her får du 100 nøje udvalgte sikkerhedstips, der gør dit digitale liv meget mere sikkert.

Journalister
Martin Lorentsen
Henning Rasmussen

Det skorter desværre ikke på dårlige nyheder, når det handler om vores brug af digitale hjælpemidler som pc og telefon. I takt med at vi er blevet mere og mere afhængige af elektronisk udstyr, er det kun gået den forkerte vej med svindleres forsøg på at udnytte den afhængighed.

Cyberangreb udgør i dag en større trussel mod vores hverdag end nogensinde før. Og med udbredelsen af kunstig intelligens er tendensen kun blevet forværret – for nu har professionelle svindlere fået et slagkraftigt værktøj, der hjælper dem med at automatisere deres kriminalitet.

Omfattende svindel

Vi har allerede set talrige eksempler på, at kunstig intelligens misbruges til at lave falske videoer, falske stemmer og forfalskede tekster med henblik på at franarre intetanende ofre følsomme data som adgangskoder og betalingsoplysninger.

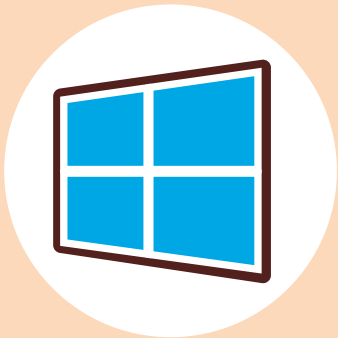
Men selv om svindlerne i stigende grad udnytter den nye teknologi til nye svindelnumre, bliver de gammeldags metoder også stadig brugt. Identitetstyveri, hvor dine Facebook-billeder og oplysninger om dig bliver brugt til at skabe en falsk person som led i et andet svindelnummer, er stadig udbredt. Ligeledes risikerer du stadig at blive snydt og købe katten i sækken, når du handler på nettet. Og svindlerne er bestemt heller ikke stoppet med at bombardere din e-mailindbakke med phishing-mails.

100 effektive sikkerhedstips

Desværre er vi som ofre næsten altid et skridt bagefter de kreative kriminelle. Alligevel kan du gøre meget for at minimere risikoen for angreb, men det kræver, at du ved, hvad du skal gøre. Her får du derfor 100 effektive sikkerhedstips, der skærmer dig bedst muligt mod alle nutidens trusler.

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

E-mail



Windows

Netværk

Kodeord

Programmer

Mobil

Facebook

Browser

Onlinehandel

1

Brug stærke adgangskoder

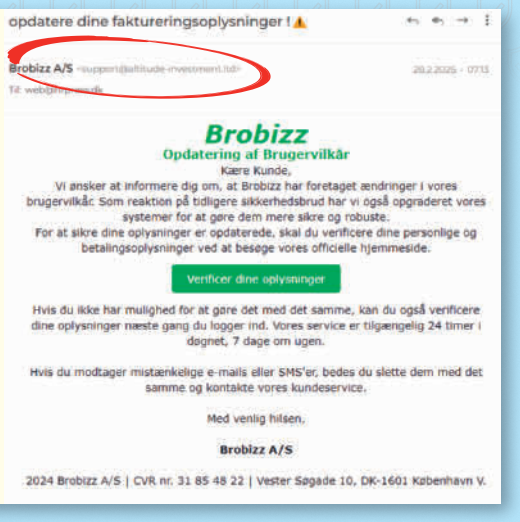
Det allervigtigste værn mod kriminelle, der kan misbruge din e-mailkonto, er, at du har sikret den med en stærk adgangskode. Ved hjælp af udspekulerede programmer forsøger hackere og svindlere konstant at få adgang til e-mailkonti på nettet, men må opgive, hvis adgangskoden er for svær. Læs mere her: **komputer.dk/2513**

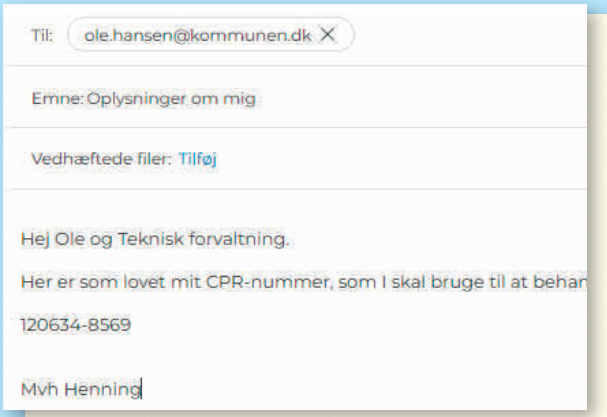
2

Tjek afsenderen, når du modtager mails

De falske e-mails er blevet så vellignende, at det ofte kun er små detaljer, der afslører dem som svindel. Vær derfor særligt opmærksom på den adresse, der vises som afsender.

Når du nærstuderer feltet med afsenderens adresse, er det ofte et helt andet firma, end mailen angiver.





En e-mail er ikke den rette kommunikationsform, hvis du har behov for at sende personfølsomme oplysninger til myndigheder eller virksomheder.

3

Del ikke alt via usikre e-mails

Helt almindelige e-mails, som du modtager og sender, er usikre, fordi indholdet ikke er krypteret. Send derfor aldrig følsomme personoplysninger som CPR-nummer, en kopi af dit pas eller lignende per e-mail, men brug i stedet en sikker løsning.

4

Lad dig ikke narre af dygtige svindlere

På engelsk kaldes det social engineering, når kriminelle fx narrer ofre til at tro, at de har modtaget en mail fra en søn eller datter, som har brug for akut økonomisk hjælp til at løse et problem. Det er svindlerne blevet så gode til, at du altid selv bør kontakte afsenderen direkte, hvis nogen skriver til dig og beder dig overføre penge eller sende dem personlige oplysninger.

5

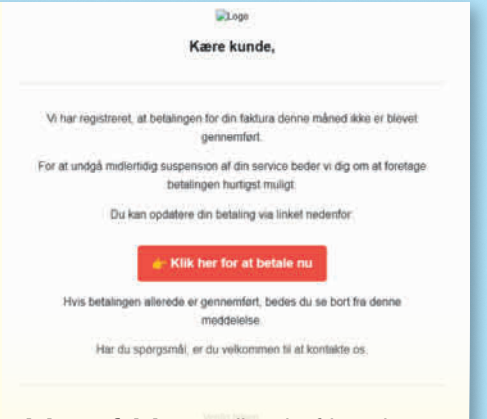
Krypter følsomme oplysninger i dine e-mails

Vi fraråder, at du bruger e-mails til at sende personfølsomme oplysninger, da mailteknologien ikke er sikker nok til formålet. Hvis du sender mails med andre oplysninger, som du heller ikke vil risikere falder i de forkerte hænder, bør du tjekke i indstillingerne for din mailkonto, om det er muligt at kryptere indholdet med teknikken S/MIME. Alternativt kan du overveje at sikre dit mailprogram med OpenPGP eller tilsvarende tjenester.

6

Klik aldrig på ukendte links

Når du modtager e-mails fra virksomheder, er de indsatte links ofte maskerede i form af knapper eller billeder, og så kan det være risikabelt at klikke på dem. Du kan afsløre, hvor en link-knap fører hen ved at holde musemarkøren over knappen – men ellers er det sikreste tip aldrig at klikke på dem.



I denne falske e-mail er det fristende at klikke på den røde knap, men linket fører til en farlig svindelside.

7

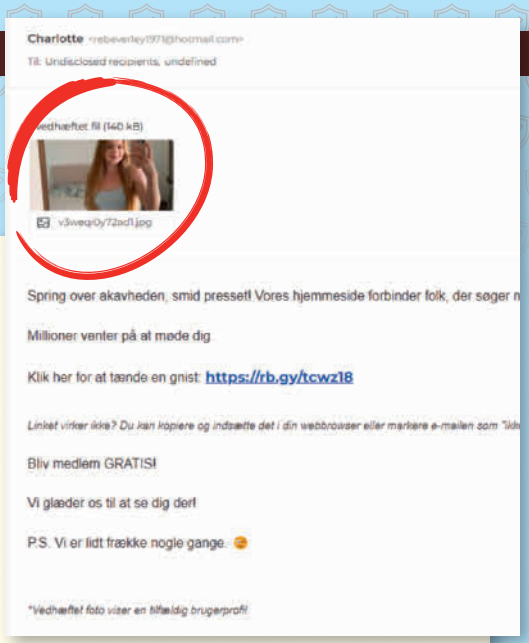
Tænd for den sikre 2-faktorgodkendelse

De fleste e-mailtjenester giver dig mulighed for den nye og sikre loginmetode, der kaldes 2-faktorgodkendelse eller totrinsverificering. Det virker på samme måde som MitID, idet du bruger en almindelig kode til første del af dit login. Herefter modtager du en engangskode. Læs, hvordan du gør på: **komputer.dk/2513**

8

Åbn ikke de vedhæftede filer

Når du modtager farlige mails fra svindlere, rummer de ofte en eller flere vedhæftede filer. Det er velkendt, at programfiler, der slutter på .exe, er farlige at afvikle, men truslen gælder faktisk også andre filtyper. De kriminelle er blevet så dygtige, at selv vedhæftede billeder kan udgøre en fare for pc'en, fordi de rummer skadelig kode.



Vedhæftede billeder i e-mails kan også være farlige at åbne på din pc.

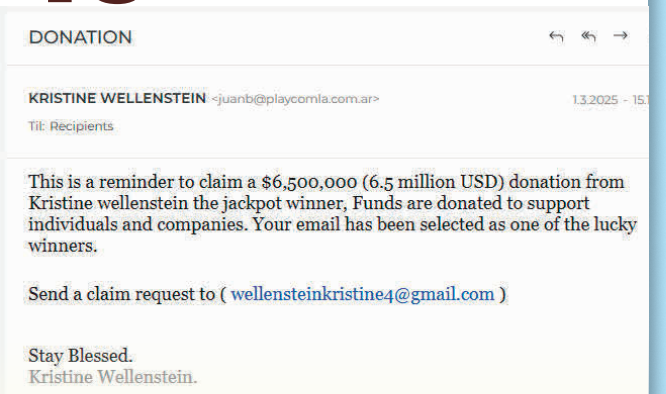
Ofte kan du høre på sproget i de falske e-mails, at der er tale om en dårlig oversættelse.

9

Tjek afsenderens sprog og tone

Der er ikke noget usædvanligt i at modtage e-mails fra fragtfirmaer som DAO eller GLS, hvis du ind imellem køber ting på nettet. Men før du følger mailens anvisninger, bør du nærstudere sproget. Det afslører ofte svindlernes dårlige oversættelser.

10



Selv om det kan lyde fristende med en økonomisk gevinst, bør du altid være skeptisk, hvis du ikke kender afsenderen.

Vær skeptisk, hvis du slet ikke kender afsenderen

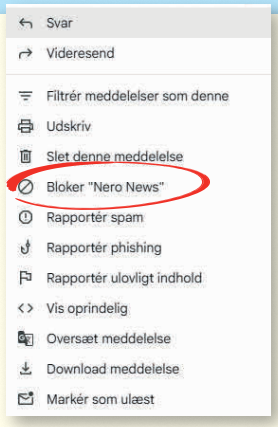
Det er som om, den menneskelige natur tilsiger, at en del af vores naturlige skepsis slås fra, når vi lokkes med store løfter. Ihvertfald har blandt andet nigerianske svindlere i årevis haft succes med et nummer, hvor de narrer ofre til at tro, at der står en større portion kontanter og venter på dem, fordi de – overraskende for alle – er i familie med en afdød velhaver.

Sådan et løfte kan naturligvis friste de fleste, men hvis navnet på afsenderen er helt ukendt for dig, fraråder vi, at du overhovedet indleder en dialog. Hvis du først begynder at svare på de falske e-mails, kan du hurtigt blive viklet ind i et farligt spind af løgne, hvor du alligevel ender med at afgive penge eller oplysninger.

11

Sæt et filter på de uønskede e-mails

Alle legitime firmaer, der sender dig nyhedsbreve og andre e-mails, giver dig også mulighed for nemt at afmelde e-mails fra firmaet. Hvis du modtager e-mails fra andre afsendere, som du ikke ønsker, kan du slippe for dem ved at oprette et filter i mailtjenester som Gmail. Se hvordan på: **komputer.dk/2513**

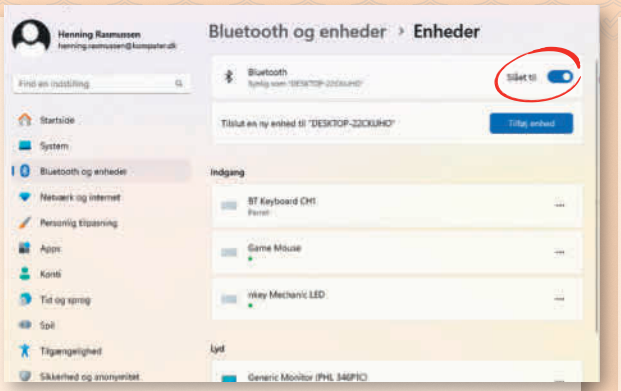


Hvis det ikke er muligt at afmelde visse mails, kan du i stedet blokere dem.

12

Slå Bluetooth fra, når du ikke bruger det

Bluetooth er en fantastisk, trådløs teknologi, der nemt forbinder fx et headset med din pc. Men teknikken kan også bruges af kriminelle, så slå Bluetooth fra, når du ikke bruger forbindelsen.

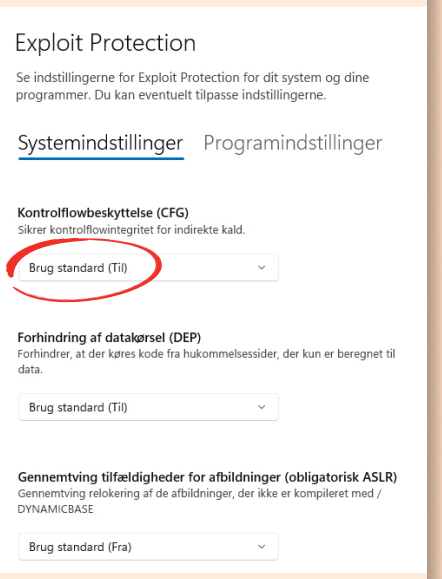


Inde i Windows' indstillinger kan du nemt slukke og tænde for Bluetooth-forbindelsen. Når den er slået fra, kan du ikke findes af andre enheder.

13

Beskyt pc'en mod farlig udnyttelse

Windows 10 og 11 rummer stærke, indbyggede sikkerhedsfunktioner, der hjælper dig med at holde din pc sikker. En af disse er **Exploit Protection**, der beskytter dig mod, at skadelig kode kan udnytte sårbarheder i pc'en.



Tjek, at **Kontrolflowbeskyttelse** er slået til inde i Windows' indstillinger under **Exploit Protection**.

14

Hold Windows opdateret

Det sker næsten altid på det mest upassende tidspunkt, at Windows beder dig fuldføre en opdatering ved at genstarte pc'en. Alligevel må vi anbefale, at du takker ja, når styresystemet beder dig installere en opdatering. Det skyldes, at Microsoft udsender vigtige sikkerhedsrettelser til din pc, som sørger for at lukke aktuelle sikkerhedshuller, der ellers lynhurtigt vil blive udnyttet af skruppelløse kriminelle.

15

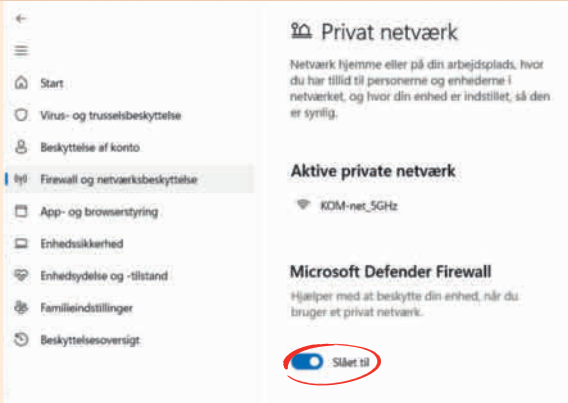
Tag regelmæssige backups af dine filer

Selv om du kan forhindre de fleste ulykker, når du følger vores 100 tips, kan du stadig være uheldig at blive ramt af malware eller ransomware, som skader eller krypterer dine filer. Sker det, er der kun én farbar vej til at se dine filer igen: Du skal bruge din sikkerhedskopi af filerne, så du kan genindlæse dem på pc'en – fx med Hasleo Backup Suite fra **komputer.dk/2513**

16

Filtrer trafikken med en firewall

En firewall er en vigtig komponent i din sikkerhed ved pc'en. Alle programmer og funktioner, som bruger netværket eller internettet, skal først passere firewallen i Windows, og det øger din sikkerhed. Tjek derfor i indstillingerne, at du har en aktiv firewall på pc'en.



Inde i Windows' indstillinger finder du panelet **Windows Sikkerhed**. Her kan du se, om firewallen på din pc fungerer, som den skal.

17

Skift til en lokal konto

Hvis du er nervøs for udvekslingen af oplysninger om din brug af pc'en på tværs af internettets servere, kan du vælge at anvende en lokal brugerkonto på din pc i stedet for en Microsoft-konto. Med en Microsoft-konto udveksles der oplysninger mellem din pc og Microsofts servere, så du fx kan synkronisere indstillinger på tværs af pc'er. Sådan opretter du en lokal konto: **komputer.dk/2513**

18

Inde i Windows Sikkerhed viser grønne flueben, at pc'en ikke er truet, og at dit antivirusprogram kører som det skal.

Tjek at dit antivirus er aktiv

Det vigtigste sikkerhedsprogram på din computer er dit antivirusprogram, der konstant holder øje med alle de filer, du henter fra internettet, og de programmer, du starter på maskinen. Derfor er det også helt afgørende, at programmet er opdateret med de nyeste virusdefinitioner, og at det kører og beskytter dig aktivt i baggrunden.

Det kan du tjekke ved at åbne **Windows Sikkerhed** fra indstillingerne i Windows. Derefter klikker du på feltet **Virus- og trusselsbeskyttelse**.

19

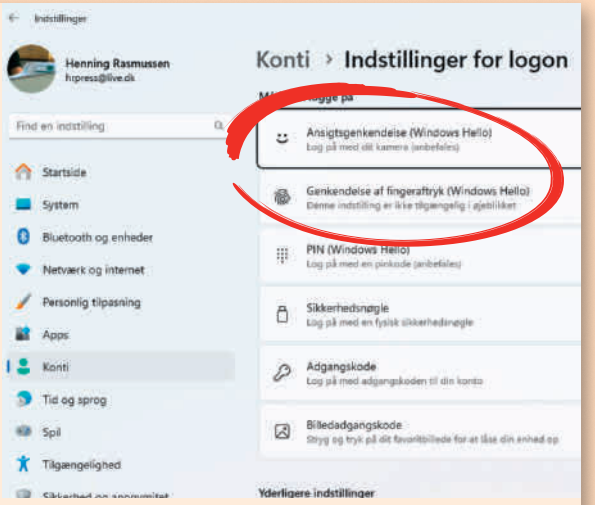
Undgå at bruge forældede programmer

Det kan måske virke som en ubetydelighed, om du lige har fået hentet den nyeste udgave af et program, men det er tværtimod afgørende for din sikkerhed. Kriminelle er dygtige til at finde nye sikkerhedshuller i kendte programmer. Det undgår du ved at holde programmerne opdaterede med de nyeste sikkerhedsrettelser fra producenten.

20

Drop koden til Windows

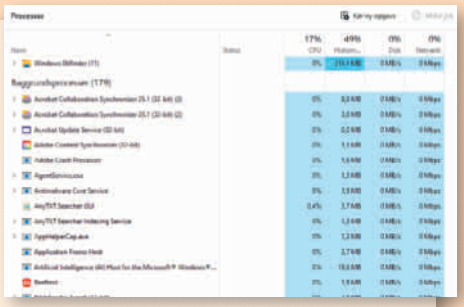
I Windows giver funktionen **Windows Hello** mulighed for, at du kan logge på pc'en med ansigtsgenkendelse eller dit fingeraftryk. Disse er meget sværere at forfalske end at gætte din kode.



I indstillingerne under **Konti og Indstillinger for logon** kan du vælge at logge på med ansigt og finger.

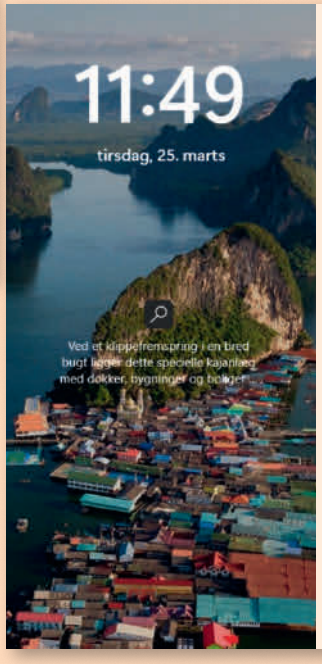
21

Tjek hvad der kører i baggrunden



Du åbner **Joblisten** ved at trykke på **Ctrl + Shift + Esc** samtidig på computerens tastatur.

Når et program eller en tjeneste kører på din pc, vil du kunne se det i **Windows Jobliste**. Her kan du også få et overblik over alle de programmer, som kører i baggrunden, og som ikke har et ikon liggende på proceslinjen. Selv om de fleste baggrundstjenester kommer fra Windows selv og har navne, der ikke nødvendigvis siger dig noget, er det stadig en god idé at tjekke oversigten ind imellem. Hvis du opdager mistænkelige navne, bør du scanne pc'en for virus og malware.



22

Lås pc'en, når du forlader den

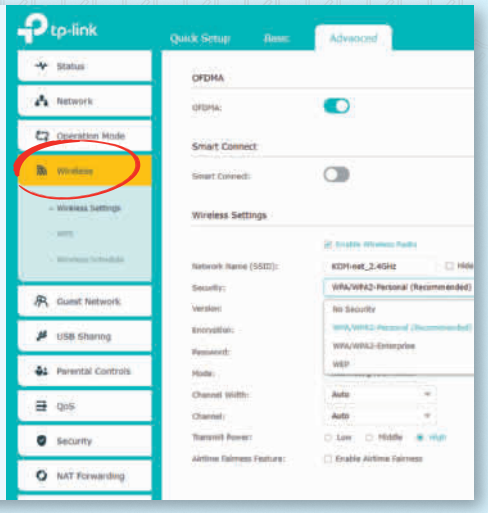
Hvis din pc aldrig forlader dit hjem, er der nok ikke stor risiko for at fremmede sætter sig ved den og snuser i dine filer. Men har du den fx med på rejse eller café, bør du låse den, når du forlader den – også selv om du kun forlader den kortvarigt.

I Windows skal du blot trykke på **Windows-tast + L** for at skifte til låseskærmen. Brug din kode for at logge ind igen.

23
Brug den bedste kryptering

Inde i din routers indstillinger kan du vælge mellem forskellige typer af kryptering af det trådløse signal. Vi anbefaler de nyeste standarder: WPA2 eller WPA3. Læs i manualen til din router, hvordan du kommer ind og ændrer indstillingerne.

I routere fra TP-Link skal du vælge **Advanced** og herefter **Wireless**.

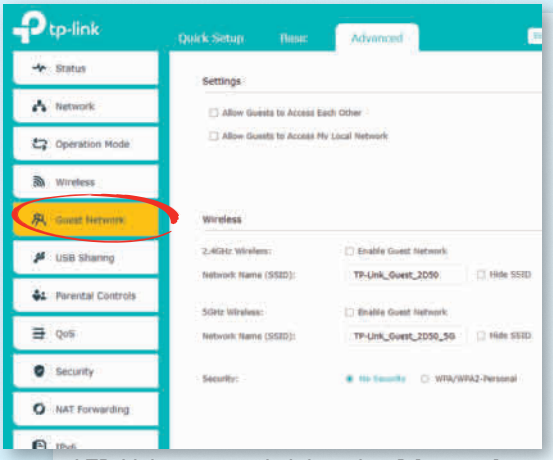


24
Luk portene i din router

Forskellige porte i din router sørger for, at du kan få adgang til udstyr i hjemmet, når du ikke er hjemme. Men har du ikke behov for dette, bør du lukke portene. Tjek i manualen til din router, hvordan du logger ind på den og finder oversigten over åbne porte.

25
Lav et særligt netværk til gæster

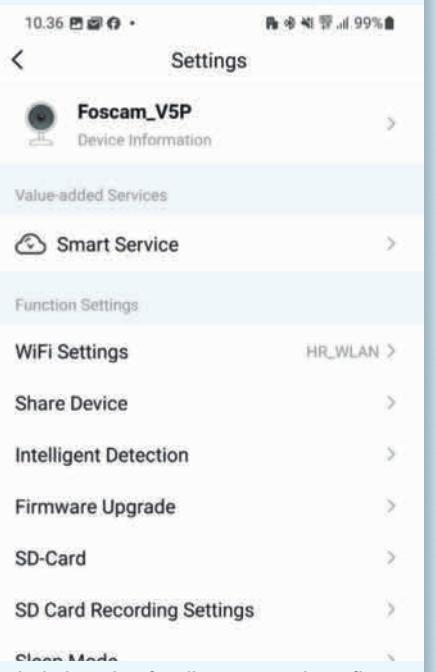
De fleste nyere routere giver mulighed for at oprette et ekstra trådløst netværk, som du kan tilbyde dine gæster. På dette netværk er der ikke adgang til andre enheder på netværket, så gæstenetværket er perfekt til at dele internetforbindelsen. Læs i manualen til din router, hvordan du opretter et gæstenetværk på din model.



I TP-Links routere skal du vælge **Advanced** og derefter **Guest Network**.

26
Hold dine smarte enheder opdaterede

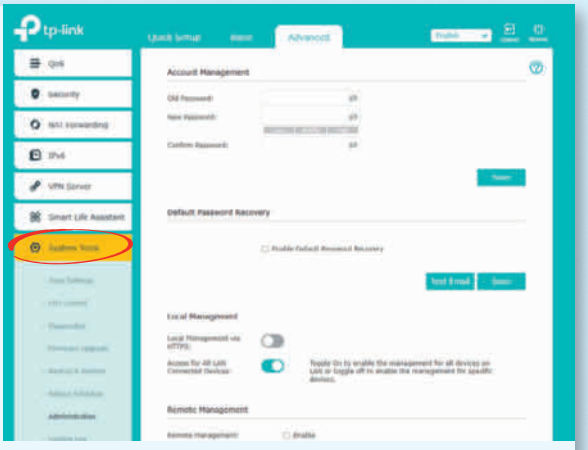
Smarte enheder som stikkontakter og kameraer kan udgøre en sikkerhedsrisiko for alle enheder på dit netværk. Det kan du undgå, hvis du sørger for at holde det smarte udstyr opdateret med firmwareopdateringer. Det gør du direkte fra enhedernes egne apps.



Inde i app'en for dit smarte udstyr finder du også muligheden **Firmware Upgrade,** hvor du kan opdatere det.

27
Sluk for fjernstyring af routeren

Har du nogensinde haft behov for at få adgang til din router, når du ikke var hjemme? Hvis ikke, er der heller ingen grund til, at funktionen er aktiv på din router. Tjek derfor i routerens manual, hvordan du slår det fra.

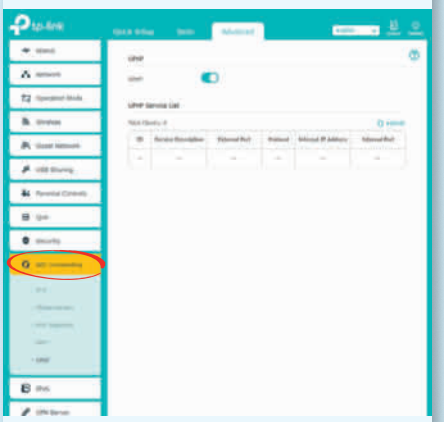


I routere fra TP-Link skal du via **Advanced** og **System Tools** for at deaktivere fjernadgang.

28

Deaktiver UPnP i din router

Routerfunktionen UPnP, som du kan læse mere om på adressen komputer.dk/2513, var egentlig designet til at gøre det lettere at forbinde forskelligt udstyr med hinanden på hjemmenetværket. I praksis har det dog siden vist sig, at funktionen også gjorde det betydeligt nemmere for kriminelle at få adgang til dit netværk. Derfor anbefaler vi, at du finder frem til funktionen via manualen til din router, og derefter logger ind og får den slået helt fra.



Funktionen UPnP finder du ofte i routerens avancerede menu under punktet **NAT Forwarding**.

29

Brug en stærk Wi-Fi-kode

Bruger du simple udtryk eller talrækker som adgangskode til dit trådløse netværk, inviterer du nærmest uvedkommende til at benytte det. Det samme gælder, hvis du ikke har ændret producentens standardkode, som fulgte med routeren. Læs derfor i routerens manual, hvordan du skifter kode på det trådløse netværk.

30

Hold din router opdateret

Det er vigtigt, at du holder alt dit udstyr opdateret: Pc, telefon og elektroniske enheder i hjemmet. Det samme gælder for din router, der løbende modtager sikkerhedsrettelser fra producenten. Tjek derfor jævnligt inde i din routers indstillinger, om der skulle være kommet en ny opdatering. Det foregår typisk fra menuen System.

31

Sluk for routerens WPS-funktion

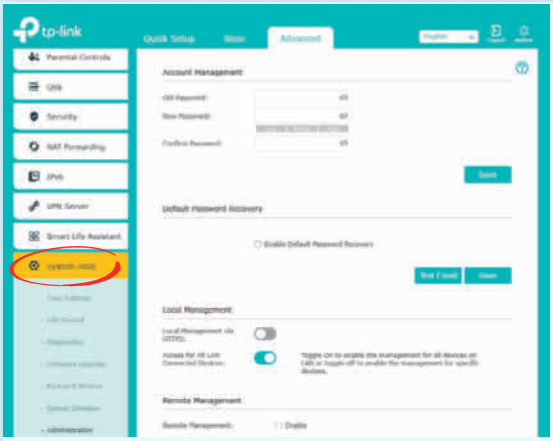
WPS findes både på din router og på det trådløse udstyr, du kan tilslutte til netværket. WPS gør det muligt at forbinde udstyr ved at trykke på en knap, men kan også misbruges. Slå den derfor helt fra.

Inde i din router har du mulighed for at deaktivere WPS-funktionen, hvis du ikke bruger den.

32

Lad ikke det trådløse netværk være tændt altid

Hvis du bor tæt på andre mennesker, vil I kunne se hinandens trådløse netværk. Selv om et ubudent besøg på netværket kræver, at fremmede har gættet din kode, kan du minimere risikoen ved helt at slukke routeren om natten.



Du skal som regel ind i menuen **System** i din router for at ændre standardkoden til at logge ind på den.

33

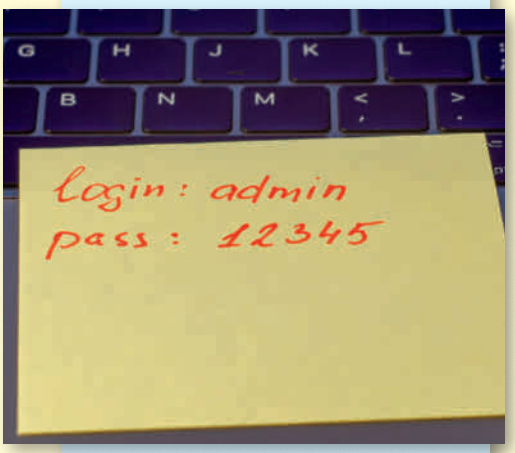
Skift koden på din trådløse router

Du skal indtaste en kode og ofte også et brugernavn, før du kan ændre indstillinger i routeren. Derfor er det vigtigt, at det er en kode, som du selv har valgt. Følg de bedste og opdaterede råd om sikre koder og skift så koden inde fra routerens egne indstillinger.

34

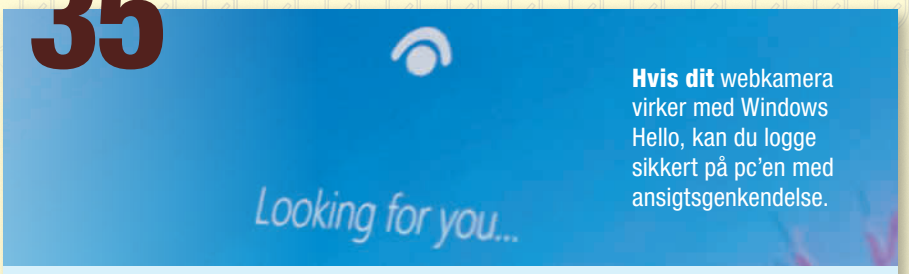
Drop de alt for indlysende koder

Det er fristende at lave koder, der er lette at huske, fordi vi lever i en tid, hvor man bruger koder til et væld af tjenester. Men fordi der konstant er mennesker med lav moral, som forsøger at få adgang til andres konto, må du ikke gøre koden for let at gætte for hverken mennesker eller avancerede programmer. Sørg derfor for at undgå koder med logiske talrækker eller almindelige ord. Læs mere her: **komputer.dk/2513**



De mest indlysende koder er alt for lette at gætte for uvedkommende. Undgå derfor talrækker og ord, du kan finde i en almindelig ordbog.

35



Hvis dit webkamera virker med Windows Hello, kan du logge sikkert på pc'en med ansigtsgenkendelse.

Log på med din finger eller ansigtet

Du kan lette antallet af besværlige koder, du skal huske på, hvis du erstatter koder med biometri, hvor det er muligt. I Windows og på din telefon kan du vælge ansigtsgenkendelse eller fingeraftryk som et alternativ til den klassiske adgangskode – og det er faktisk mere sikkert.

36

Gør dine kodeord ekstra lange

Jo længere en adgangskode er, desto længere tid vil det tage for en computer at bryde den eller en kriminel at gætte den. Derfor anbefaler de fleste sikkerhedseksperter nu koder på mindst 12 tegn og gerne flere.

37

Find på remser

Du kan gøre din sikre og lange kode nemmere at huske, hvis du forbinder den med noget, der betyder noget for dig. Det kunne fx være en remse eller en sang, der er blandet med tegn, tal og store bogstaver i stil med 1Rose!SåJeg$kyde.

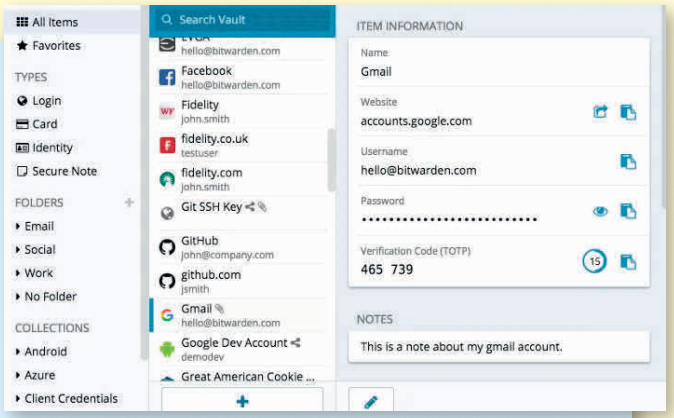
38

Genbrug aldrig dine kodeord

Selv om det kan lette mængden af koder, du skal huske, bør du aldrig genbruge dine adgangskoder på tværs af forskellige tjenester. Det kan nemlig i værste tilfælde betyde, at du giver kriminelle fri adgang til alle tjenesterne, hvis de får opsnappet koden til én af tjenesterne.

39

Få hjælp til at huske alle koderne



Bitwarden Free er en udmærket kodeordshusker, der holder styr på alle de sikre adgangskoder.

Hvis du allerede nu synes, det kan være svært at huske hverdagens mange adgangskoder, bliver det kun værre efterhånden som koderne skal være længere og mere besværlige. Den byrde kan du lette ved at anvende en såkaldt password-manager. Det er et smart program, som du åbner med en hoved-adgangskode, og så sørger programmet for at holde styr på alle de svære enkeltkoder. Du kan fx bruge programmet Bitwarden Free, som du finder i vores sikkerhedspakke på **komputer.dk/2513**.

40

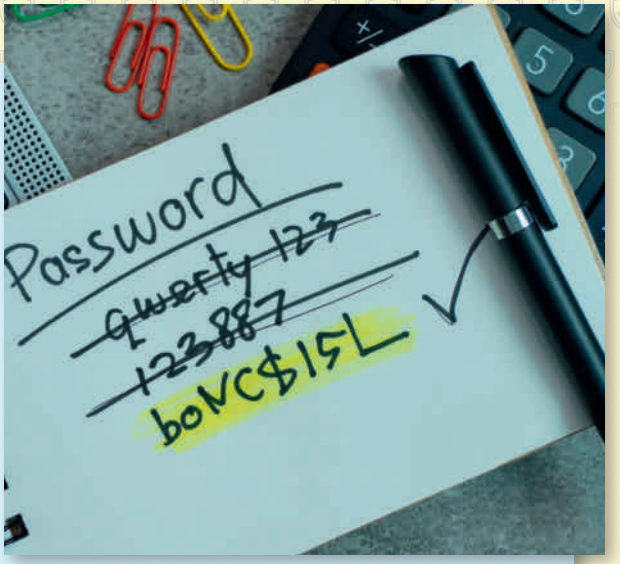
Er dine koder lækket på nettet?

Ind imellem sker der store datalæk, hvor hackere lænser tjenester for oplysninger om tilmeldte brugere. I mange tilfælde får de kriminelle også adgang til folks e-mailadresser og adgangskoder, og så er det naturligvis risikabelt, hvis du bruger samme login på andre tjenester. Du kan selv tjekke, om dine oplysninger er lækket ved at gå i Chromes indstillinger, vælge **Privatliv og sikkerhed** og **Gå til Sikkerhedstjek**.

41

Lav en god blandingskode

Opskriften på en god og stærk adgangskode har mindst fire sikre ingredienser: Din kode skal både bestå af store og små bogstaver – gerne spredt tilfældigt i koden. Og så skal du huske besværlige specialtegn som @, !, % og lignende, der ikke nemt kan gættes, og tilfældige tal. Læs mere: komputer.dk/2513



Drop de logiske tal- og bogstavrækker og skab i stedet en kode, der umiddelbart virker tilfældig.

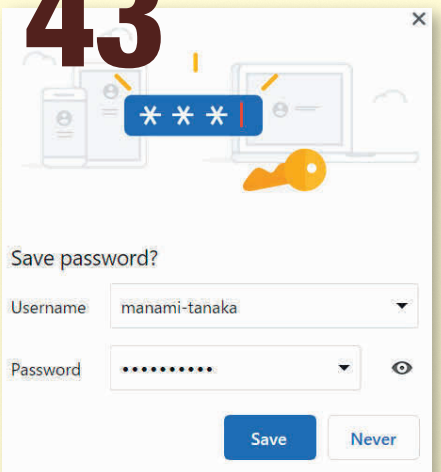
Med totrinsverificering skal du også bruge en tilfældig engangskode.

42

Dobbeltsikring er mere effektivt

Der er en grund til, at Danmarks officielle loginsystem, MitID, både kræver et personligt login og en fysisk enhed i form af din telefon med en app, hvor du godkender. Det er ganske enkelt mere sikkert end en løsning, der kun består af den ene del. Du kan få samme høje sikkerhed på din mail ved at aktivere totrinsverificering i tjenesten.

43



Din foretrukne browser er flink til at foreslå at gemme koder til hjemmesider for dig, men det er ikke uden risiko.

Browseren bør ikke gemme dine koder

Det er fristende at takke ja, når browsere som Edge og Chrome foreslår at gemme koden til en hjemmeside for dig, men det er ikke ligeså sikkert som at bruge en rigtig kodeordsmanager. Det skyldes, at der normalt er fri adgang til at se koderne for folk, der låner din pc, og at koderne ikke er beskyttet særligt godt mod hackere.

44

Hundens navn er for usikkert

Du tænker måske, at fremmede aldrig vil kunne gætte din adgangskode, selv om du har brugt navnet på dit kæledyr eller et barnebarn i den. Når det frarådes af eksperter, skyldes det også i højere grad, at navne og rigtige ord kan "gættes" ved ordbogsopslag, udført af specialprogrammer.

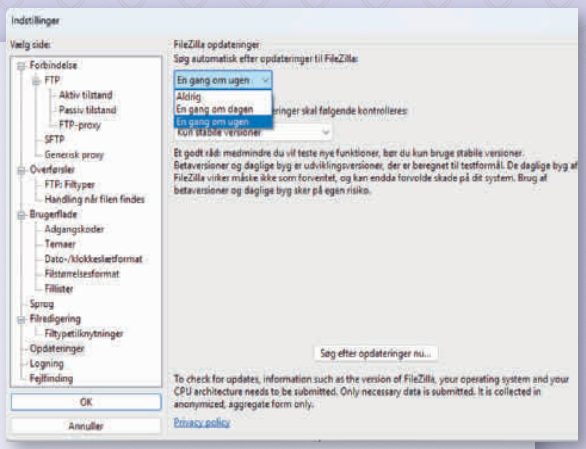
Navne på kæledyr er strengt forbudt i dine adgangskoder, da det gør dem alt for nemme at gætte.

45
Undgå falske download-sider

Det er ikke uden risiko at anvende en søgetjeneste som Google til at finde og hente et program på nettet. Ofte risikerer du at lande på en falsk download-side, hvor du måske tror, at du henter et rigtigt program, men ender med virus på maskinen. Derfor bør du kun hente programmer direkte fra producenten eller på **komputer.dk**, hvor vi scanner det hele for virus.

46
Lad programmerne opdatere sig selv

Programmer, der står uopdaterede hen i årevis, er notorisk usikre, fordi hackere har haft god tid til at finde sikkerhedshuller i dem. Det undgår du ved at sørge for, at dine programmer er opdaterede. I de fleste programmer er det endda muligt at indstille dem til selv at lede efter og installere nye opdateringer.



Inde i indstillingerne for de fleste programmer er det muligt at aktivere automatiske opdateringer. Du kan fx få programmet til at tjekke en gang om ugen.

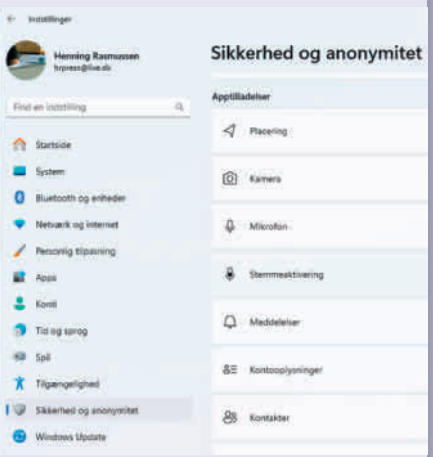
Her er vi ved at installere programmet doubleTwist, da Delta Toolbar pludselig dukker op.

47
Undgå ekstra godter i installationerne

Du skal være på vagt, når du installerer programmer på pc'en. Især de gratis programmer er slemme til at tilføje andre valgfrie programmer i installationen, fordi det giver producenten en lille ekstraindtægt. Nærlæs derfor, hvad du accepterer under installationen, og afslå hvad du ikke kender.

48
Tjek, hvad dine programmer har lov til

Har du lyst til, at et program fra en mindre producent kan se din placering eller tænde dit webkamera? Hvis ikke, kan du gennemgå programmernes tilladelser: Højreklik på startknappen i Windows, og klik på **Indstillinger**. Klik derefter på **Sikkerhed og anonymitet**, vælg en tilladelse – fx **Placering** – og se, hvilke af dine programmer, der har lov til at se oplysningerne.



I Indstillinger under **Sikkerhed og anonymitet** kan du se tilladelserne for dine installerede programmer har.

49
Fjern alle overflødige programmer på pc'en

Hvis du har haft din pc i længere tid, har du formentlig også installeret mange programmer på den gennem tiden – også programmer, du ikke længere bruger. Disse programmer kan udgøre en sikkerhedsrisiko, og derfor bør du gennemgå **Indstillingerne** og fjerne programmer. Læs mere her: **komputer.dk/2513**

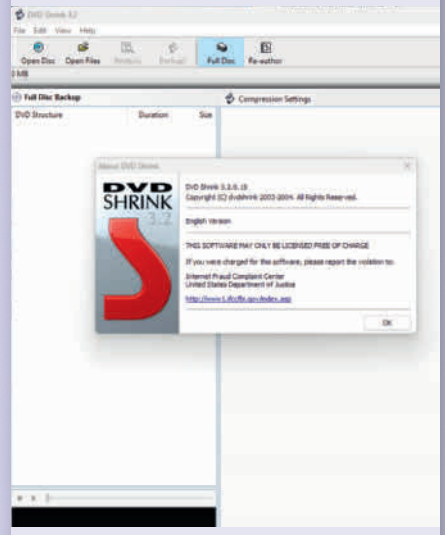
50
Kører der farlig ransomware på pc'en?

Hvis pc'en virker sløvere end normalt, kan der være skadelige programmer, som arbejder i det skjulte. De frygtede ransomware-infektioner lægger fx stort beslag på harddisken, når programmerne krypterer dine filer for at afkræve en løsesum. Det kan du tjekke i Joblisten ved at trykke på **Ctrl + Shift + Esc**. Tjek så fanen **Disk**.

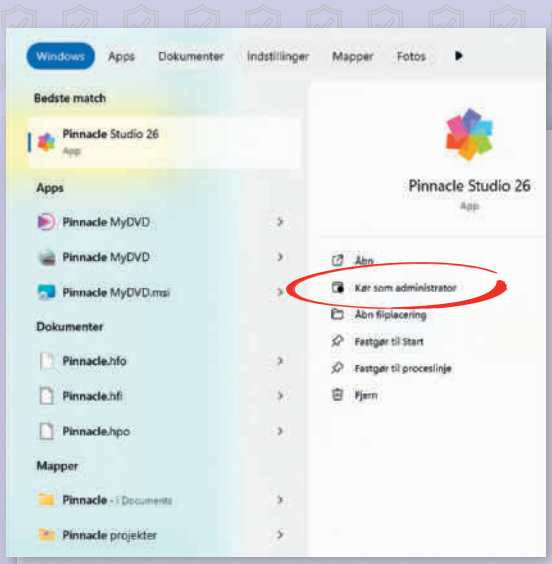
51

Modtager programmet stadig opdateringer?

Selv gode programmer bliver ind imellem forladt af producenten, og så er det slut med opdateringer. Dermed får du heller ikke lappet sikkerhedshuller, og så bliver det risikabelt at fortsætte med at bruge det forladte program. Derfor bør du tjekke, hvornår dine programmer senest er opdaterede.



DVD Shrink er et godt program til at gemme dvd-film på harddisken, men det modtog sin sidste opdatering i 2004 og er derfor usikkert at bruge.



Søgeresultaterne i startmenuen giver dig mulighed for at køre programmer som administrator.

52

Giv ikke uhindret adgang til pc'en

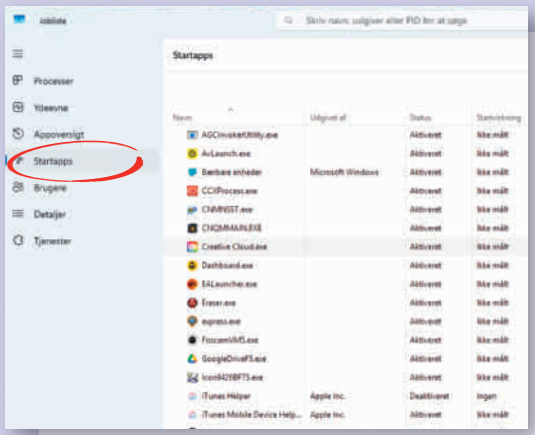
Når du søger programmer frem i startmenuen eller højreklikker på en genvej, har du mulighed for at køre programmer som administrator. Det bør du aldrig gøre medmindre programmet kun virker med den indstilling. Administratoradgang giver nemlig programmerne langt flere beføjelser på din pc.

53

Giv hellere filerne et ekstra tjek

Du kan ikke altid stole ubetinget på dit antivirusprogram, når det frikender et program eller en fil. Vil du være helt sikker, må du høre en uvildig tredjepart. Vi anbefaler hjemmesiden virustotal.com, hvor du kan uploade filer, og få svar på, hvordan de vurderes af alle førende sikkerhedsprogrammer på markedet.

På VirusTotal skal du blot klikke på **Choose file**, vælge en fil på harddisken, og så får du straks klar besked, om filen er farlig.



På fanen **Startapps** inde i **Joblisten** kan du se de programmer, der starter med Windows.

54

Begræns programmer, der selv starter

De små programmer, der starter automatisk sammen med Windows, er ikke kun belastende for pc'ens ressourcer. Der kan også skjule sig ondsindede programmer blandt startprogrammerne. Tag derfor et kritisk blik på fanen **Startapps** i Joblisten, som du åbner med **Ctrl + Shift + Esc**.

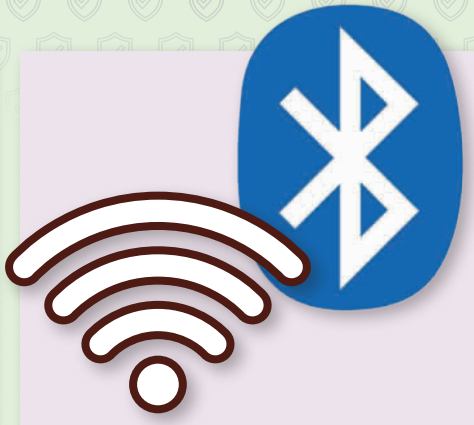
55

Giv programmerne begrænset adgang til computeren

Ransomware er en virustype, der først krypterer dine filer for bagefter at afkræve dig penge for at låse dem op igen. Men hvis virussen ikke har adgang til dine filer, kan den ikke kryptere dem. Lås derfor mapperne med funktionen **Styret mappeadgang** i indstillinger.

56
Installer antivirus

Hvis du bruger iPhone, er du allerede godt beskyttet, men hvis du har en Android-mobil, er det en rigtig god idé at beskytte dig med et antivirusprogram – ligesom du gør på pc'en. Sophos Intercept X for Mobile er den bedste gratis antivirus-app til Android, og på vores hjemmeside viser vi, hvordan du bruger den. Find artiklen via dette link: **komputer.dk/2513**



Der er ingen grund til, at hverken Wi-Fi eller Bluetooth er slået til, når du ikke bruger de trådløse forbindelser.

57
Sluk Bluetooth og Wi-Fi

Wi-Fi og Bluetooth er smarte trådløse forbindelser, men de kan også være vejen ind for hackere på din mobil. Du bør kun have Wi-Fi slået til, når du er på trådløse netværk, du stoler på. Bluetooth bør du kun have aktiveret, når du skal bruge et trådløst headset eller højtalere. Når du ikke bruger forbindelserne, kan du nemt slå dem fra midlertidigt i mobilens indstillinger.

58
Hold din telefon opdateret

Der kan løbende opstå sikkerhedshuller i softwaren til din mobil, som hackere står i kø til at udnytte. Derfor bør du sikre dig, at telefonens styresystem er opdateret. Du kan altid tjekke, om der er en opdatering klar ved at åbne din iPhones eller Android-mobils indstillinger og gå til kategorien, der omhandler softwareopdateringer eller oplysninger om telefonen.

I mobilens indstillinger om telefonen kan du klart og tydeligt se, om alt er opdateret.

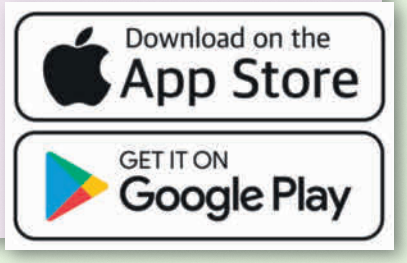
59
Vælg et godt hotspot-kodeord

Du kan dele din telefons data og logge på nettet på en anden enhed via mobilens internetdeling. Det kaldes et mobilt hotspot. Gør du det, er det vigtigt, at du beskytter dit mobile hotspot med en god adgangskode. Du skifter koden inde i indstillingerne, hvor du også aktiverer det mobile hotspot. Husk at bruge små og store bogstaver samt specialtegn og tal i koden.

60
Hent kun apps fra officielle butikker

Den nemmeste vej ind på din mobil for en hacker er via apps. Ofte dukker der falske, farlige apps fyldt med malware op, som fx kan føre til, at din mobilbank bliver lænset, eller at du bliver overvåget. Hvis du henter apps fra officielle app-butikker, mindsker du risikoen for at blive inficeret.

På iPhone skal du hente apps fra App Store. På Android skal du bruge Play Butik.



61

Er dine apps ikke opdaterede, bliver det lettere for hackere at inficere dem med malware.

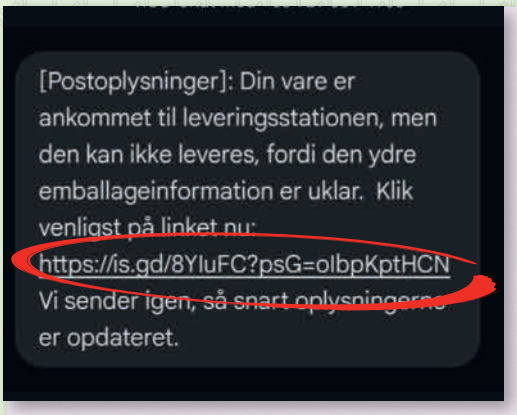
Opdater dine apps

Ligesom du skal holde din mobils styresystem opdateret for at styrke sikkerheden, skal du huske at opdatere telefonens apps med jævne mellemrum. Så kan du bruge dine apps med ro i sindet. Læs, hvordan du opdaterer apps på **komputer.dk/opdater-apps**

62

Tag backup af dine billeder

I dag gemmer de fleste af os billeder på telefonen, for det er med mobilen, at vi tager vores fotos. Sker der noget med din telefon, kan du dog risikere at miste dine billeder, hvis ikke du har gemt dem et andet sted også. Derfor bør du tage backup af dine billeder i ny og næ. Læs, hvordan du bedst gør det her: **komputer.dk/2513**



Typisk er svindelbeskeden udstyret med et link, som du opfordres til at trykke på.

63

Pas på svindel i sms-indbakken

Ligesom tilfældet er i din e-mail-indbakke, vil du modtage svindel i sms-indbakken. Det kan fx være en sms om en mislykket levering af en pakke som vist på skærmbilledet her. Det kan også være falske beskeder fra myndighederne eller beskeder, om at du har vundet en præmie.

64

Undgå offentlige USB-stik

Hvis du støder på en offentlig USB-opladestation, kan det være fristende at sætte mobilen til, men det bør du være påpasselig med. Hackere bruger nemlig USB-stikkene til at installere malware på din telefon. Metoden kaldes for "juice jacking" og går ud på at stjæle dine oplysninger.

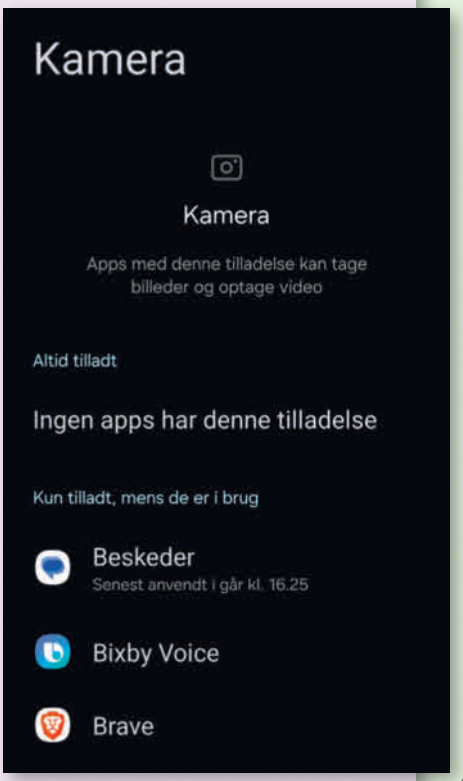
65

Tjek dine apps' tilladelser

Du bør gennemgå, hvilke apps der har adgang til mobilens værktøjer. På en Samsung-mobil finder du oversigten med tilladelser i kategorien **Apps**, hvor du skal trykke på de tre prikker og vælger **Tilladelsesstyring.** Metoden kan variere en smule, hvis du har en anden telefon, men typisk skal du ind i indstillingerne for apps for at finde oversigten med tilladelser, hvorfra du nemt kan deaktivere de uønskede tilladelser.

Det er især tilladelser ved mikrofonen, GPS, kameraet, opkald og sms-beskeder, du skal være opmærksom på.

Der bør ikke være nogle apps, der altid har tilladelse til fx at bruge mobilens kamera. Ser du det, skal du fjerne tilladelsen.



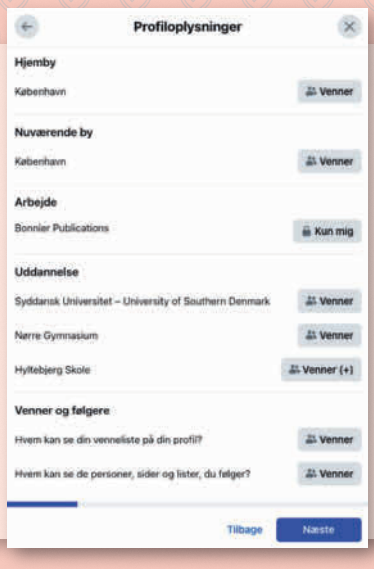
66

Lås mobilen med biometri

Biometri på mobilen, som fingeraftryk eller ansigtsgenkendelse, giver dig mulighed for hurtigt at låse din telefon op uden at bruge en kode. Og så er det en sikker måde at beskytte data med, for det kræver dine unikke fysiske træk, hvis mobilen skal låses op.

I din mobils sikkerhedsindstillinger kan du aktivere de biometriske funktioner.

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



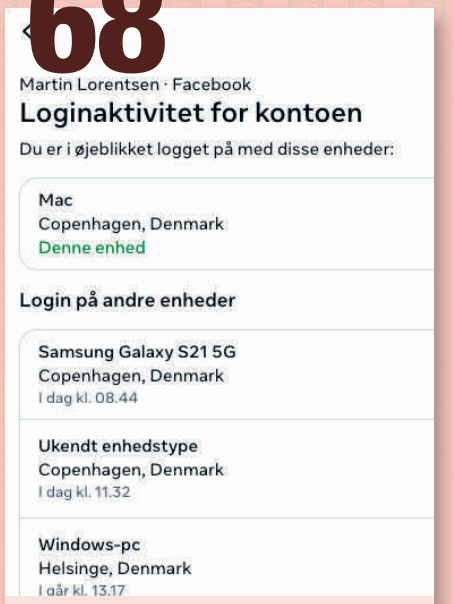
67

Gør din profil privat

Du kan gøre din profil privat og mindske risikoen for identitetstyveri ved at klikke på dit profilbillede øverst til højre på Facebook og derefter vælge **Indstillinger og privatindstillinger**. Vælg **Kontrol af privatindstillinger**, og gennemgå kategorierne på siden.

Du bør sørge for, at det enten kun er dig eller dine venner, der kan se dine oplysninger på Facebook.

68



Ser du en enhed, som du ikke kan genkende, klikker du på de tre prikker ud for enheden og vælger **Log ud**.

Tjek hvor du er logget ind

Har du mistanke om, at andre har adgang til din profil, kan du tjekke det. Klik på dit profilbillede øverst til højre, og vælg **Indstillinger og privatindstillinger**. Klik derefter på **Aktivitetslog** efterfulgt af **Hvor du er logget på**. Så ser du alle steder, du er logget på.

69

Pas på falsk indhold

På Facebook har man droppet at faktatjekke, og derfor vrimler det efterhånden med falsk indhold på tjenesten. Desværre er det falske indhold ikke bare løgnagtigt, det kan også være decideret farligt at klikke på det. Fx kan et link til en falsk artikel føre til en svindelside, hvor du bliver franarret følsomme oplysninger, eller du kan risikere at installere virus. Vær ekstra kritisk, når du læser opslag på Facebook.

70

Husk at logge af

Måske lyder det banalt, men du skal huske at logge af Facebook, når du ikke bruger tjenesten. Det gælder især, hvis du har været logget ind på en offentlig computer eller på en pc, du deler med andre. Ellers risikerer du, at uvedkommende får adgang til din profil.

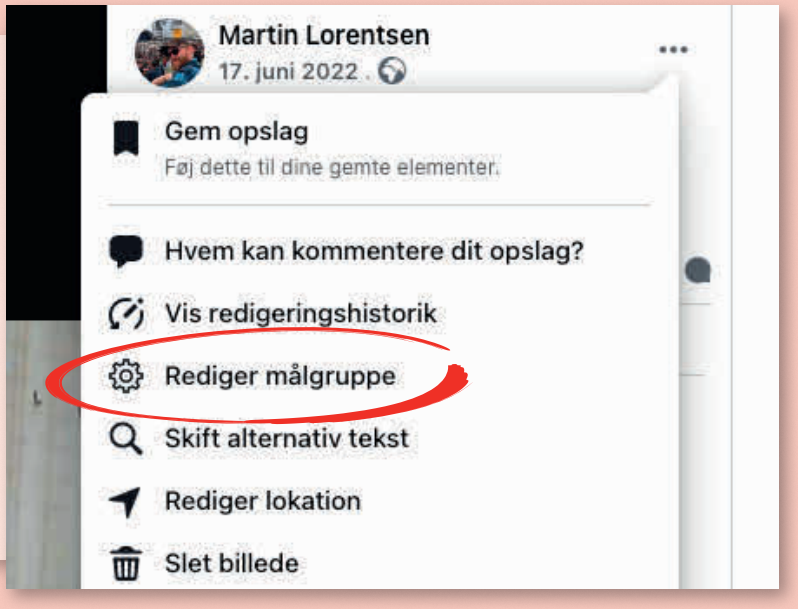
Når du er logget af, skal du tjekke, at browseren ikke har gemt din e-mail og dit kodeord. Har den det, skal du sørge for at fjerne det.

71

Gør profilbilledet privat

Svindlere elsker at bruge Facebook til at stjæle tilfældige ofres identitet og bruge den til at svindle andre. På mange Facebook-profiler er der nemlig fri adgang til profilbilleder, som svindlerne nemt kan gemme på pc'en og misbruge. Du kan forhindre dette ved at gøre dit profilbillede privat, så kun du og dine venner kan åbne fotoet. Andre kan stadig se billedet, men kun i miniatureformatet, og det kan hackerne ikke bruge til meget.

Åbn dit profilbillede, og klik på de tre prikker. Klik på punktet **Rediger målgruppe**, og vælg så dine venner.

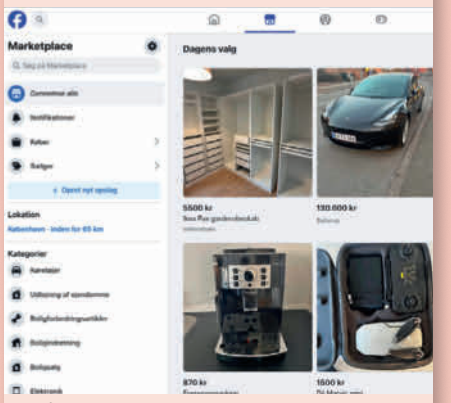


72

Vær forsigtig på markedspladsen

Facebook Marketplace er navnet på Facebooks markedsplads, hvor du kan købe og sælge brugte varer. Men der er adskillige eksempler på, at både købere og sælgere er blevet svindlet.

Fx vil en sælger tilbyde mærkevarer som Apple-produkter eller designertøj til unaturligt lave priser, men i virkeligheden sælge en kopi eller intet. Et andet eksempel er købere, der vil betale via tvivlsomme tjenester, hvor du ikke kommer til at se skyggen af dine penge. Desuden kan du risikere at købe stjålne varer.



På Facebook Marketplace skal du være særligt kritisk, når du handler.

73

Pas på links i Messenger

Får du en besked ud af det blå på Facebooks chattjeneste Messenger, hvor du opfordres til at klikke på et link, skal du være skeptisk. Det gælder især, hvis du får en besked fra en fremmed, men alarmklokkerne bør også ringe, hvis en af dine Facebook-venner er afsender. Der kan være svindlere på spil, som har hacket din vens profil.

Sker det, bør du kontakte din ven ad andre veje end Messenger for at høre, om vedkommende har sendt beskeden med linket eller ej.

74

Tænk over hvad du deler

Facebook er designet til, at du skal dele dine oplevelser og indtryk med venner og familie, men tænk alligevel over, hvad du egentlig deler med andre.

Hvis du ikke har en privat profil, kan hvem som helst i princippet se, hvad du deler og bruge dine oplysninger mod dig. Det gælder ikke kun, hvad du skriver i statusopdateringer, men i høj grad også, hvad der står om dig på din profil. Overvej at skjule disse private oplysninger. Læs, hvordan du gør det her: **komputer.dk/2513**

75

Slå underretninger til

I Facebooks indstillinger kan du aktivere en funktion, så du får besked, hvis nogen får adgang til din konto fra en usædvanlig placering. Så kan du hurtigt reagere og logge vedkommende ud igen. Derefter skal du straks ændre din adgangskode.

Funktionen findes i privatindstillingerne ved at klikke på **Kontrol af privatindstillinger** og derefter vælge **Sådan beskytter du din konto**.

76

Bliv kun venner med folk du kender

Modtager du en venneanmodning fra en person, du ikke kender eller ikke har mødt, bør du holde igen med at acceptere anmodningen. Især hvis du ikke har nogle fælles venner med vedkommende. Det kan i disse tilfælde være en svindler. Læs, hvordan du opdager en falsk profil her: **komputer.dk/2513**

I indstillingerne for beskyttelse af din konto kan du skifte din adgangskode eller aktivere totrinsgodkendelsen.

77

Brug totrinsverifcering

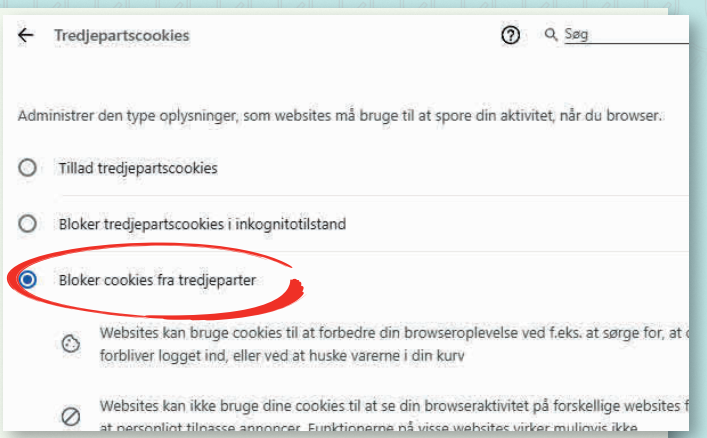
Totrinsgodkendelse på Facebook kræver, at du indtaster en kode fra din mobil, udover din adgangskode, når du logger ind. Det gør det sværere for hackere at få adgang til din konto. Du kan aktivere totrinsgodkendelsen i sikkerhedsindstillingerne.

78

Ryd de snagende cookies

Cookies kan gemme dine præferencer på de hjemmesider, du besøger ofte, så det bliver hurtigere at indlæse siderne, men cookies bruges også til at spore dig på tværs af hjemmesider. Særligt tredjepartscookies skal du være opmærksom på, for det er andre end den hjemmeside, du besøger, der står bag disse cookies.

Cookies fra tredjeparter stammer som regel fra reklamefirmaer, der sporer din færden på nettet med henblik på at overlæsse dig med reklamer, der er målrettet dig på baggrund af din online-aktivitet. Det vil sige, at de reklamer, der dukker op på hjemmesider, vil relatere sig til, hvad du tidligere har foretaget dig på nettet, og det kan være indgribende i forhold til dit privatliv.



Google Chrome og de fleste andre browsere kan du sætte en stopper for de sporende tredjepartscookies. I Chromes tilfælde sker det under **Privatliv og sikkerhed**-indstillingerne.

I Chrome kan du tjekke tilladelser ved at åbne indstillingerne for privatliv og sikkerhed og vælge **Websitedsindstillinger**. Du kan derefter gennemgå tilladelserne og se de hjemmesider, der har fået tilladelse.

79

Gennemgå tilladelser

Mange hjemmesider beder om adgang til din computers komponenter som kamera, mikrofon og placering, mens andre hjemmesider vil have lov til at sende dig notifikationer i browseren. Du bør regelmæssigt gennemgå og justere disse tilladelser, så du ikke giver hjemmesider unødvendigt mange friheder.

80

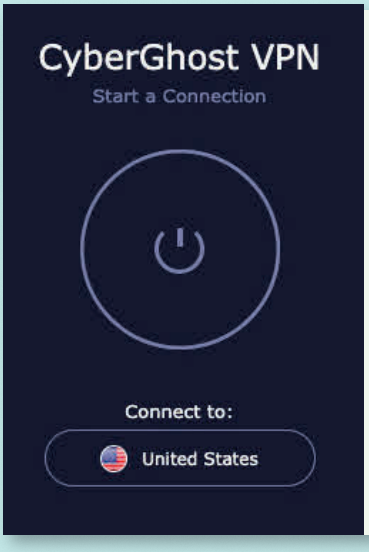
Luk browseren regelmæssigt

At have browseren kørende i dagevis kan både belaste pc'en og medføre potentielle sikkerhedsrisici. Når du lukker browseren, slettes visse midlertidige filer og sessionscookies, som ellers kan udnyttes af hackere til at overvåge dig. Gør det til en vane at lukke browseren dagligt.

81

Fjern gemte kodeord

Det kan virke praktisk at lade browseren huske dine adgangskoder, men det udgør en sikkerhedsrisiko. Hvis din computer eller Google-konto – såfremt du bruger Chrome som din browser – bliver kompromitteret, kan uvedkommende nemt få adgang til dine logins. På vores hjemmeside viser vi, hvordan du fjerner de gemte kodeord fra både Chrome og Edge-browseren: **komputer.dk/2513**



82

Brug en VPN

En VPN krypterer din internetforbindelse og skjuler din IP-adresse. Det gør det sværere for hjemmesider og hackere at overvåge dig. De fleste VPN-tjenester koster penge, men du kan installere udvidelsen CyberGhost VPN Free Proxy gratis. Læs, hvordan du bruger udvidelsen her: **komputer.dk/2513**

Med den gratis browserudvidelse CyberGhost VPN Free Proxy får du en glimrende VPN til Chrome og Firefox, så du kan skjule din IP-adresse.

83
Klik ikke på reklamer

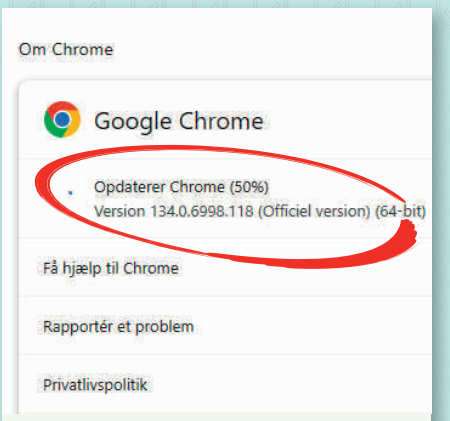
Reklamer på hjemmesider kan være mere end bare irriterende. Nogle reklamer er nemlig lavet til at føre dig til skadelige hjemmesider eller installere malware på din pc. Disse annoncer forsøger eksempelvis at lokke dig til at klikke på dem med falske advarsler eller tilbud på produkter eller pc-programmer.

Selv tilsyneladende legitime reklamer kan være snyd, og derfor bør du undgå at klikke på reklamerne, medmindre du er helt sikker på, hvem der står bag.

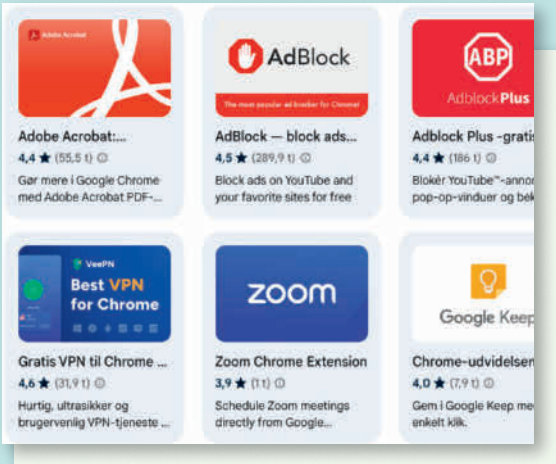
84
Pas på hvad du downloader

Mange sikkerhedsproblemer begynder med en uforsigtig download fra nettet. Undgå at hente filer fra ukendte eller utroværdige kilder. Og er du i tvivl, bør du altid scanne filer, du henter, med dit antivirusprogram.

Vær særligt opmærksom på hjemmesider, der lokker med gratisudgaver af ellers dyre programmer til pc'en. Husk, at hvis noget virker for godt til at være sandt, er det nok også tilfældet.



Bruger du Chrome kan du tjekke, om browseren er opdateret under **Om Chrome**-kategorien i indstillingerne.



Hold øje med anmeldelserne af udvidelserne, når du skal hente dem fra fx Chrome Webstore.

85
Tjek udvidelser grundigt

Browserudvidelser kan gøre meget godt for dig, men de kan også være skadelige. Tjek derfor, hvilke udvidelser du har installeret, og fjern de ubrugte. Undersøg desuden anmeldelser og udgiverens troværdighed. Læs, hvordan du fjerner udvidelser her: komputer.dk/2513

86
Hold browseren opdateret

Gamle versioner af browsere har – ligesom meget andet software – ofte sikkerhedshuller, som hackere kan udnytte.

Sikkerhedshullerne bliver lappet, når browseren bliver opdateret, og de fleste browsere, fx Google Chrome og Microsoft Edge, opdateres automatisk. Det kræver dog, at du manuelt genstarter browseren ved at lukke den ned og åbne den igen.

87
Brug en sikker browser

Nogle browsere, fx Firefox og Brave, har fokus på privatliv og sikkerhed og giver dig som standard bedre kontrol over, hvad der bliver delt med tredjeparter. Brave blokerer for sporingscookies og reklamer automatisk, mens Firefox har avancerede indstillinger for privatlivskontrol. Begge browsere kan hentes her: komputer.dk/2513

Brave og Firefox er gode at bruge, hvis du vil beskytte privatlivet bedre, når du er på nettet.

88
Vær opmærksom på domænesnyd

Phishing-angreb sker ofte via domæner, der ligner kendte sider, men med små variationer – fx "faceboook.com" i stedet for "facebook.com". Tjek altid domænet nøje, før du logger ind eller downloader noget. Et enkelt besøg på den forkerte side kan give en hacker adgang til dine oplysninger.

89
Gå efter e-mærket

E-mærket er en certificering, der gives til webbutikker, som lever op til en række krav om sikkerhed, gennemsigtighed og forbrugerbeskyttelse. Når du handler på en side med e-mærket, har du ekstra garanti for, at dine rettigheder bliver respekteret. Du har også adgang til gratis juridisk hjælp ved eventuelle tvister. Gå derfor efter det, især når du handler nye steder.

E-mærket ser ud som vist her, og typisk kan du finde det nederst eller øverst på butikkens hjemmeside.

90
Brug ikke en offentlig pc

Offentlige computere, fx på biblioteker eller hoteller, kan være udsatte. Når du handler online, indtaster du ofte følsomme oplysninger som betalingsoplysninger og adresser, og det vil du næppe have, at andre får adgang til. Brug altid din egen pc, når du shopper på nettet, og sørg for, at den er opdateret og har antivirus installeret.

91
Læs betingelserne grundigt

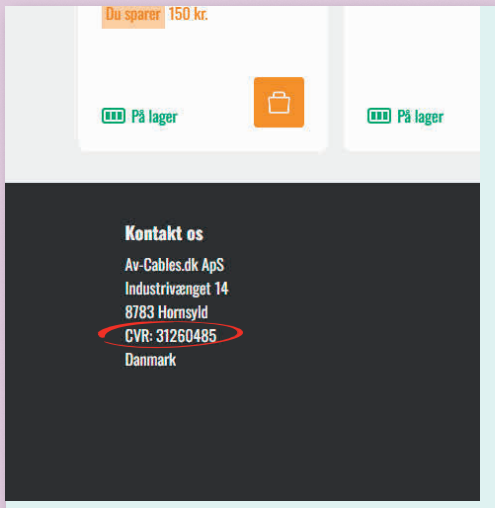
Mange klikker hurtigt "godkend", uden at læse handelsbetingelserne, men de indeholder vigtige oplysninger som regler om returret, leveringstider og gebyrer. Især ved køb fra udlandet kan der gemme sig ekstra omkostninger eller dårligere forbrugerbeskyttelse. Brug lidt tid på at læse betingelserne, så du ved, hvad du siger ja til.

92
Undersøg butikkens adresse

En troværdig webbutik oplyser altid sin fysiske adresse. Hvis adressen mangler, eller den ser mystisk ud, bør du være på vagt. Brug Google Maps til at tjekke, om adressen eksisterer og matcher firmaets profil. Mange svindelbutikker bruger fiktive adresser eller henviser til kontorhoteller, og så er der ugler i mosen.

93
Betal med MobilePay

MobilePay er en hurtig og sikker betalingsmetode, når du går på indkøb på internettet. Dine kortoplysninger bliver nemlig ikke delt med webbutikken, når du bruger Mobile Pay, og da du godkender betalingen via din telefon, har du bedre kontrol med betalingerne. Desuden registreres transaktionen tydeligt i din app og i banken, så du har dokumentation ved eventuelle problemer. Brug derfor MobilePay, når det er muligt.



Webbutikken vil vise CVR-nummeret enten i bunden eller i toppen af hjemmesiden.

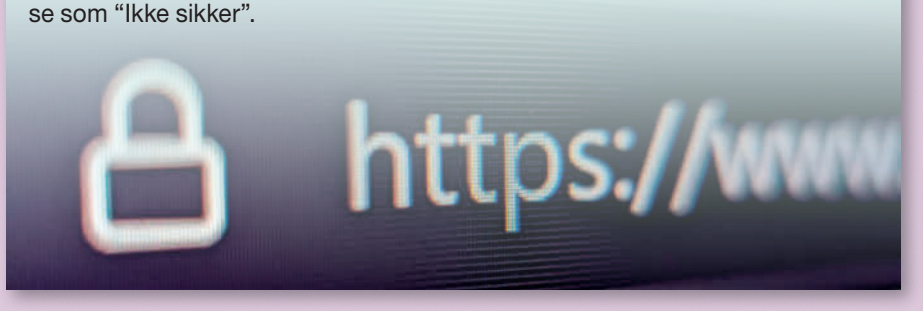
94
Tjek virksomhedens CVR-nummer

En hurtig og effektiv måde at tjekke, om du handler med en reel forhandler, er at tjekke virksomhedens CVR-nummer, som du kan finde på butikkens hjemmeside. Et CVR-nummer er et firmas officielle registrering i Danmark. Ved at slå det op på **virk.dk**, kan du se, om virksomheden eksisterer, og hvem der står bag. Et manglende eller falsk CVR-nummer er typisk et tegn på svindel.

Med MobilePay får butikken ikke dit kortnummer, så hvis forretningen bliver hacket, skal du ikke være nervøs.

95
Køb kun fra hjemmesider med https

Står der "https", og er der en hængelås i adresselinjen, betyder det, at forbindelsen mellem dig og webshoppen er krypteret. Det beskytter dine oplysninger mod at blive opsnappet af tredjeparter. Hvis siden kun bruger "http", bør du undgå at indtaste personlige data, og det gælder især kreditkortoplysninger. I dag markerer de fleste browsere hjemmesider uden en sikker forbindelse som "Ikke sikker".



96
Tjek altid anmeldelser

Brugeranmeldelser på Trustpilot kan give dig en idé om, hvordan virksomheden behandler sine kunder. Kig både på karakteren og selve kommentarerne. Tjek især de dårlige anmeldelser. Hvis andre har haft problemer med levering, kundeservice eller returret, bør du være ekstra forsigtig.

Søg efter butikken på Trustpilot, og tjek anmeldelserne grundigt.

97
Pas på private handler

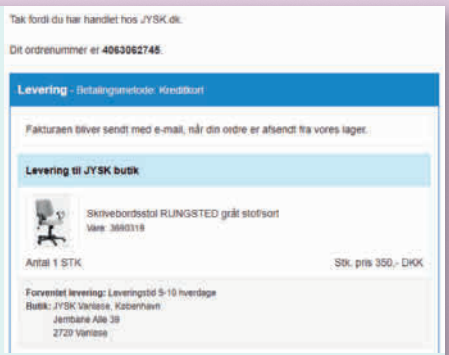
Når du handler med private, fx på DBA, har du ikke samme forbrugerbeskyttelse som ved køb fra en webshop. Du bør aldrig overføre penge på forhånd, medmindre du stoler fuldt ud på sælgeren. Mød gerne den anden part fysisk, og betal først ved modtagelse af varen. Skal varen sendes, bør du bruge sikre betalingsløsninger med mulighed for tilbageførsel.

98
Gennemgå din bankkonto efter køb

Efter onlinekøb er det en god vane at tjekke dine banktransaktioner. Sørg for, at det beløb, du har godkendt, stemmer overens med det, der er trukket. Uautoriserede eller dobbelte hævninger kan være tegn på fejl eller misbrug. Hvis du opdager noget mistænkeligt, skal du straks kontakte din bank. Jo hurtigere du reagerer, desto bedre.

99
Gem ordrebekræftelsen

Gem altid ordrebekræftelsen, når du har handlet. Den kommer ofte enten som e-mail eller PDF og fungerer som dokumentation for, hvad du har købt, hvornår, og til hvilken pris. Det er nyttigt ved retur og reklamation, eller hvis varen aldrig dukker op. Sørg for at gemme ordrebekræftelsen et sikkert sted, så du altid kan finde den igen.


Tak fordi du har handlet hos JYSK.dk.

Dit ordrenummer er **4063062745**.

Levering - Betalingsmetode: Kreditkort

Fakturaen bliver sendt med e-mail, når din ordre er afsendt fra vores lager.

Levering til JYSK butik

Skrivebordsstol RUNGSTED grå stof/sort
Vare: 3660318

Antal 1 STK — Stk. pris 350,- DKK

Forventet levering: Leveringstid 5-10 hverdage
Butik: JYSK Vanløse, København
Jembane Alle 39
2720 Vanløse

Med en ordrebekræftelse kan du nemt dokumentere, hvad du har købt, og hvad varen kostede, hvis du får brug for det.

100
Tjek hvor der sendes fra

Det er ikke altid tydeligt, hvor en vare, du køber online, sendes fra. Mange webbutikker har dansk navn og domæne, men sender varerne fra Kina eller andre lande uden for EU. Det kan give lange leveringstider, højere fragtudgifter og risiko for told og moms. Tjek altid leveringsoplysninger i betingelserne, inden du bestiller. Det står med småt, men kan have stor betydning for dine omkostninger.

Det kan koste dig ekstra penge, hvis den vare, du køber fra nettet, bliver leveret langvejs fra.

Foto: Ryan DeBerardinis, nik_nadal/Shutterstock.com