



effektiva tips för att skydda dig

Din digitala resa på internet, i mobilen och på datorn är full av okända fallgropar. Här är 100 noggrant utvalda säkerhetstips som gör ditt digitala liv mycket säkrare.



Journalister
Martin Lorentsen
Henning Rasmussen

Tyvärr råder det ingen brist på dåliga nyheter och faror när det gäller vårt användande av digitala enheter som datorer och mobiler. I takt med att vi har blivit allt mer beroende av våra elektroniska prylar har bedragarnas försök att dra nytta av det beroendet bara accelererat i fel riktning.

Cyberattacker utgör idag ett större hot mot vår vardag än vad de har gjort någonsin tidigare. Det beror delvis på artificiella intelligensens framfart som gjort att trenden bara förvärrats,

eftersom professionella bedragare har fått ett kraftfullt verktyg som hjälper dem att automatisera sina brott.

Omfattande bedrägerier

Vi har redan sett många exempel på hur artificiell intelligens missbrukas för att skapa falska videoklipp, falska röster och förfälskade texter för att försöka lura av intet ont anande offer känsliga uppgifter som lösenord och betalningsinformation.

Samtidigt som bedragarna i allt större utsträckning använder sig av ny teknik för att skapa bedrägerier, används fortfarande gamla och väl beprövade metoder. Identitetsstöld, där Facebook-foton och Facebook-

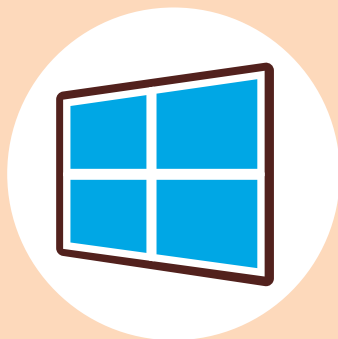
information används för att skapa en falsk personlighet som en del av ett bedrägeri, är fortfarande vanligt. På samma sätt riskerar du fortfarande att bli lurad när du handlar på nätet. Och bedragarna har verkligen inte slutat bombardera din inkorg med nätfiskemejl heller.

100 effektiva säkerhetstips

Tyvärr är vi som offer nästan alltid ett steg efter de kreativa brottslingarna. Ändå kan du göra väldigt mycket för att minimera risken för attacker, men du måste veta vad du ska göra. Här är 100 effektiva säkerhetstips som skyddar dig mot hot som du riskerar att råka ut för.



Mejl



Windows



Nätverk



Lösenord



Program



Mobil



Facebook



Webbläsare



Näthandel





1

Använd starka lösenord

Det viktigaste skyddet mot att brottslingar ska missbruka ditt mejlkonto är att skydda det med ett kraftfullt lösenord. Hackare och bedragare försöker ständigt komma åt dåligt skyddade mejlkonton på nätet med hjälp av sofistikerade program, men ger upp om lösenordet är för svårt. Läs mer här: pctidningen.se/2513

2

Titta på avsändaren när du får mejl

Falska mejl har blivit så vanliga att det ofta bara är små detaljer som avslöjar att det rör sig om bedrägerier. Var extra uppmärksam på den adress som står som avsändare.

När du studerar fältet med avsändarens adress, är det ofta ett annat företag än vad mejlet påstår.

Misstänkt aktivitet på ditt konto inloggen x

Microsoft Alert security.update@microsoft.topnet.tech till mig

Microsoft 365**Varning!**Misstänkt aktivitet på ett konto som tillhör **Jonas Svensson**.

Någon har precis loggat in på ditt Microsoft 365-konto från War

Om det inte var du som loggade in - [klicka här för att avbryta se](https://password.microsoftonline.com/) logga in på <https://password.microsoftonline.com/> och uppdater

Support Team - Microsoft Corporation (c) - Windows Security Update

Skicka

Till ole.hansen@kommunen.se

Ämne: Information om mig

Hej Ole och teknisk ledning.

Som utlovat, här är mitt personnummer som du behöver för att handlägga

120634-8569

Mh Jonas

Mejl är inte rätt kommunikationsform om du behöver skicka känslig information till myndigheter eller företag.

3

Dela inte allt via osäkra mejl

Vanliga mejl är osäkra eftersom innehållet inte är krypterat. Därför ska du aldrig skicka sådant som är känsligt, som ditt personnummer eller ett foto av ditt pass eller körkort, via mejl. Använd istället alltid en krypterad lösning som är säkrare.

4

Låt dig inte luras av skickliga skojare

På engelska kallas det för social engineering när brottslingar lurar sina offer att tro att de har fått ett mejl från en son eller dotter som behöver akut ekonomisk hjälp för att lösa ett problem. Bedragarna har blivit så duktiga på detta att du alltid ska kontakta avsändaren direkt om någon skriver till dig och ber dig att föra över pengar eller skicka personlig information.

5

Kryptera känslig information i dina mejl

Vi rekommenderar inte att du använder mejl för att skicka känslig information eftersom mejltekniken inte är tillräckligt säker. Om du ändå måste skicka mejl med information som du inte vill ska hamna i orätta händer bör du kontrollera inställningarna för ditt mejlkonto för att se om du kan kryptera innehållet med S/MIME-tekniken. Alternativt kan du överväga att skydda ditt mejlprogram med OpenPGP eller liknande tjänster.

6

Klicka aldrig på okända länkar

När du får mejl från företag är länkarna ofta maskerade så att de liknar knappar eller bilder, och det kan vara riskabelt att klicka på dem. Du kan avslöja vart en länk leder genom att bara hålla muspekaren över knappen. Annars är det klart säkraste tipset att aldrig någonsin klicka på okända länkar.

Kära kund,

Vi har registrerat att betalningen för din faktura denna månad inte har slutförts.

För att undvika tillfällig avstängning av din tjänst ber vi dig att göra betalningen så snart som möjligt.

Du kan uppdatera din betalning via länken nedan:

[Klicka här för att betala nu](#)

Om betalningen redan har genomförts, vänligen bortse från detta meddelande.

Om du har några frågor är du välkommen att kontakta oss.

I det här falska mejlet är det frestande att klicka på den röda knappen, men länken leder till en farlig bluffsida.

7

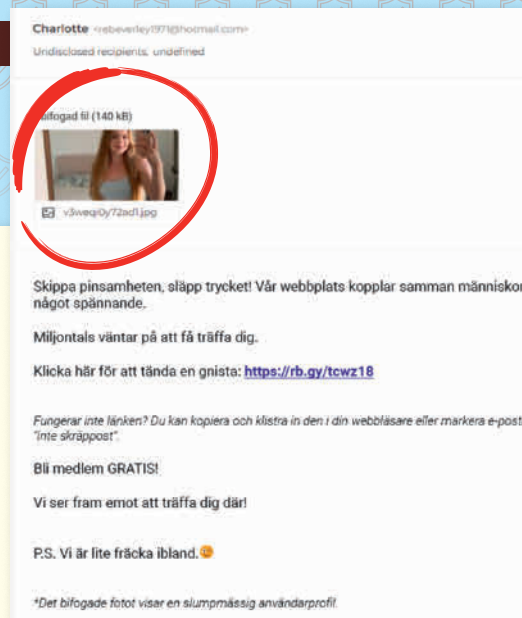
Använd alltid säker tvåfaktorausautentisering

De flesta mejltjänster tillåter dig att använda den nya och säkra inloggningsmetoden som kallas 2-faktorausautentisering eller tvåstegsverifiering. Det fungerar på samma sätt som BankID, men med en vanlig kod för den första delen av inloggningen. Därefter får du en engångskod. Läs hur du gör på: pctidningen.se/2513

8

Öppna aldrig några bifogade filer

Mejl som kommer från bedragare innehåller ofta bifogade filer. Att programfiler som slutar på .exe är kan vara farliga att köra är välkänt, men hotet sträcker sig även till andra filtyper. Brottslingarna har blivit så skickliga att även bilder som bifogas kan utgöra en fara för datorn eftersom de kan innehålla skadlig programkod.



Bifogade bilder kan också vara farliga att öppna på datorn.

9

Kontrollera språk och ton

Det är inget ovanligt att få mejl från fraktbolag som PostNord eller DHL om du handlar saker på nätet. Innan du följer mejlets instruktioner bör du dock undersöka språket. Grammatiska fel och felstavningar avslöjar ofta bedragares dåliga översättningar.



Ofta kan man se på språket i falska mejl att det rör sig om en dålig översättning.

10

DONATION



Även om kan vara frestande att bli ekonomiskt oberoende ska du vara skeptisk om du inte känner avsändaren.

Var skeptisk om du inte vet vem avsändaren är

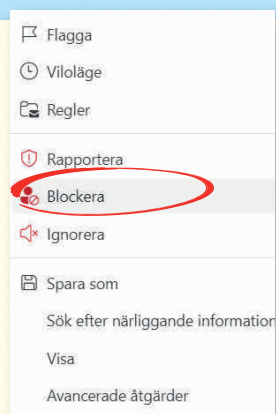
Det är som att den mänskliga naturen dikterar att en del av vår naturliga skepticism stängs av när vi lockas med storslagna löften. I årtal har svindlare genomfört ett framgångsrikt bedrägeri där de lurar offren att tro att det finns en stor summa kontanter som väntar på dem eftersom de – till stor överraskning för samtliga inblandade – är släkt med en avliden rik man.

Naturligtvis kan ett sådant löfte vara frestande för somliga, men om avsändarens namn är helt okänt för dig råder vi dig att inte ens inleda en dialog. När du väl börjar svara på de falska mejlen kan du snabbt bli indragen i en farlig härva av lögnar där du till slut ändå förlorar pengar eller information.

11

Skapa filter för oönskade mejl

Seriösa företag som skickar nyhetsbrev och andra mejl till dig ger dig också möjlighet att enkelt avregistrera dig från deras utskick. Om du får mejl från andra avsändare som du inte vill ha kan du bli av med dem genom att skapa ett filter i mejltjänster som Gmail. Läs om hur du kan göra detta på: pctidningen.se/2513

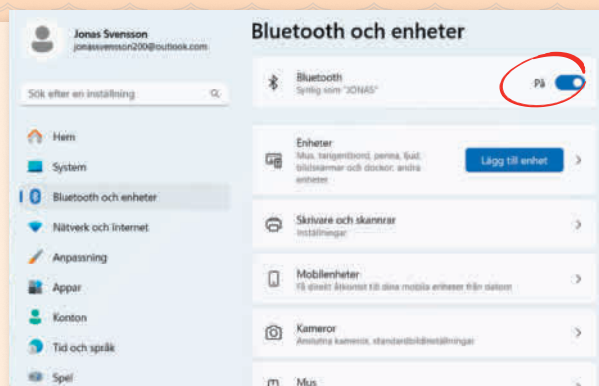


Om det inte går att avregistrera sig från vissa mejl kan du blockera dem.

12

Slå av Bluetooth när du inte använder det

Bluetooth är en fantastisk teknik för att enkelt ansluta exempelvis ett headset till datorn. Men den kan också användas av brottslingar, så stäng av Bluetooth när du inte använder anslutningen.



I **Windows-inställningar** kan du enkelt aktivera och inaktivera Bluetooth-anslutningen. När den är avstängd kan du inte hittas av andra enheter.

14

Uppdatera Windows

Det är nästan alltid vid olämpliga tidpunkter som Windows ber dig att slutföra en uppdatering genom att starta om datorn. Det bästa är trots allt att du accepterar när operativsystemet ber dig installera en uppdatering. Det beror på att Microsoft regelbundet släpper viktiga säkerhetsuppdateringar som stänger aktuella säkerhetshål som skulle kunna utnyttjas av skrupelfria brottslingar.

15

Gör regelbundna backuper av dina filer

Även om många tragedier går att undvika, kan du fortfarande råka drabbas av skadliga program och ransomware som skadar eller krypterar dina filer. Om det händer finns det bara ett hållbart sätt att rädda dina filer: Du behöver din backup så att du återställa filerna på datorn – till exempel med Hasleo Backup Suite från pctidningen.se/2513

13

Skydda din dator mot farlig exploatering

Windows 10 och 11 har starka, inbyggda säkerhetsfunktioner som hjälper dig att hålla datorn säker. En av dessa säkerhetsfunktioner är **Sårbarhetsskydd** som ser till att skadlig programkod inte kan utnyttja sårbarheter i datorn.

Sårbarhetsskydd

Visa inställningarna för sårbarhetsskydd för ditt system och dina program. Du kan anpassa inställningarna.

Systeminställningar Programinställningar

Control Flow Guard (CFG)

Säkerställer kontrollflödesintegritet för direkta anrop.

Använd standard (På)

Dataexekveringsskydd (DEP)

Förhindrar kod från att köras från minnessidor med enbart data.

Använd standard (På)

Framtvinga randomisering för avbildningar (obligatorisk ASLR)

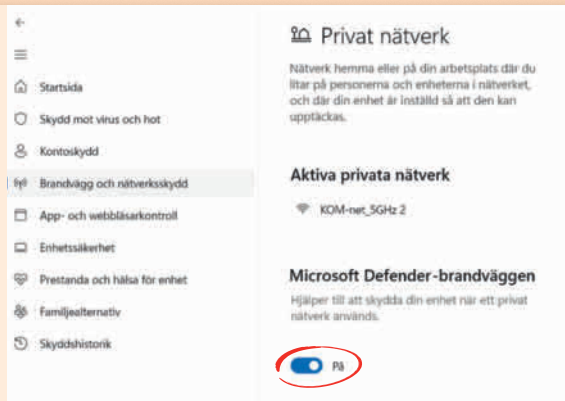
Framtvinga omplacering av avbildningar som inte har kompilerats med DYNAMICBASE

Kontrollera att **Control Flow Guard** är aktiverat i Windows inställningar under **Sårbarhetsskydd**.

16

Filtrera trafik med en brandvägg

En brandvägg är en viktig del av säkerheten i din dator. Alla program och funktioner som använder internet måste passera brandväggen i Windows, vilket ökar din säkerhet. Därför ska du kontrollera i inställningarna att du har en aktiv brandvägg på datorn.



I Windows-inställningarna hittar du avdelningen som heter **Windows-säkerhet**. Här kan du se om brandväggen på datorn fungerar som den ska.

17

Byt till ett lokalt konto

Om inte vill att information om ska spridas mellan internetserverar kan du välja att använda ett lokalt användarkonto i stället för ett Microsoft-konto. När du har ett Microsoft-konto utbyts information mellan din dator och Microsofts serverar så att du till exempel kan synkronisera inställningar mellan olika datorer och rädda lösenord. Så här skapar du ett lokalt konto: pctidningen.se/2513

18



I **Windows-säkerhet** visar gröna bockar att datorn inte är hotad och att antivirusprogrammet fungerar som det ska.

Kolla att antivirus är aktivt

Det viktigaste säkerhetsprogrammet på din dator är antivirusprogrammet, som hela tiden övervakar alla filer du hämtar från internet och de program du kör på datorn. Därför är det viktigt att programmet är uppdaterat med de absolut senaste virusdefinitionerna och att det aktivt körs och skyddar dig i bakgrunden.

Det kan du kontrollera genom att öppna **Windows-säkerhet** inställningarna i Windows. Där klickar du på kategorin **Skydd mot virus och hot**.

19

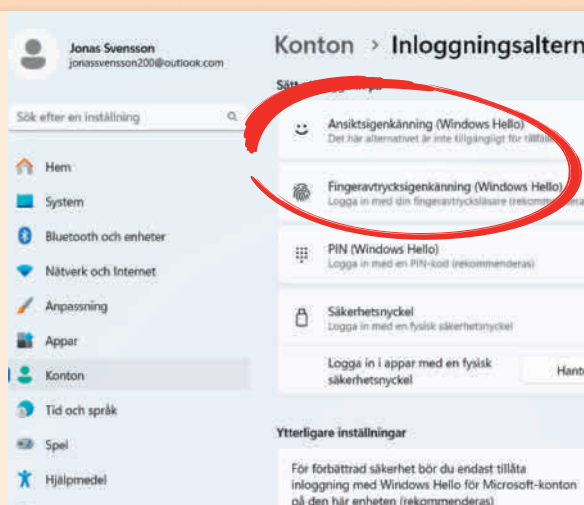
Undvik att använda föråldrade program

Det kan verka trivialt att alltid ha den senaste versionen av ett program, men det är viktigt för din säkerhet. Kriminella är skickliga på att hitta nya säkerhetshål i kända program. För att undvika detta bör du hålla dina program uppdaterade med de senaste säkerhetsuppdateringarna från tillverkaren, och inte använda program som inte längre uppdateras.

20

Logga in med ansiktet eller ett finger

I Windows finns **Windows Hello**, en funktion som gör det möjligt att logga in med ansiktsgenkänning eller fingeravtryck. Dessa är betydligt svårare att knäcka än att gissa sig till ditt lösenord.



Under **Konton** och **Inloggningsalternativ** i Windows inställningar kan du välja biometrisk inloggning.

21

Kolla vad som körs i bakgrunden

När ett program eller en tjänst körs på datorn kan du se det om du öppnar

Appar (1)	Status	18%	44%	0%	0%
Appar (1)					
Aktivitetshanteraren		14.2%	39.2 MB	0 MB/s	0 MB/s
Bakgrundsprocesser (42)					
AMD External Events Client M...		0%	2.2 MB	0 MB/s	0 MB/s
AMD External Events Service ...		0%	0.8 MB	0 MB/s	0 MB/s
AMDRSServ		0%	2.8 MB	0 MB/s	0 MB/s
Algopt Indexing Engine		0%	5.4 MB	0 MB/s	0 MB/s
Application Frame Host		0%	9.6 MB	0 MB/s	0 MB/s
AutoModeDetect		0%	1.7 MB	0 MB/s	0 MB/s
chrome		0%	8.7 MB	0 MB/s	0 MB/s
COM Surrogate		0%	1.1 MB	0 MB/s	0 MB/s

Öppna **Aktivitetshanteraren** med kortkommandot **Ctrl + Shift + Esc**.

Här kan du även få en överblick över alla program som körs i bakgrunden och men som inte har någon ikon i aktivitetsfältet. Även om de flesta bakgrundstjänster kommer från Windows självt och har namn som inte nödvändigtvis säger dig något, är det ändå en god idé att kontrollera översikten då och då. Om du upptäcker några misstänkta namn bör du skanna datorn efter virus och skadlig programvara.

22

Lås din dator när du lämnar den

Om din dator aldrig lämnar ditt hem är risken inte så stor att någon främmande person sätter sig vid den och snokar i dina filer. Om du däremot tar med dig den på resor eller till ett café bör du låsa den när du lämnar den – även om det bara är för en kort stund.

I Windows trycker du på **Windows-tangenten + L** för att växla till låsskärmen.

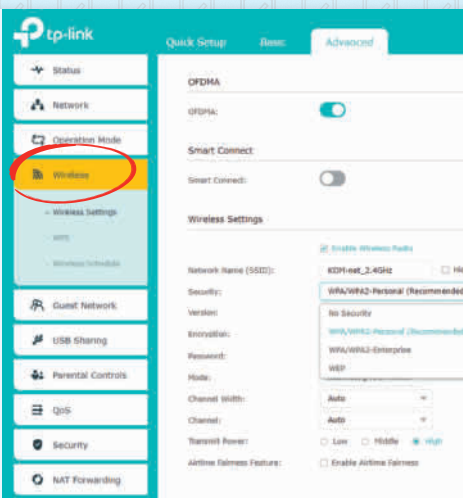


23

Använd den bästa krypteringen

I routerns inställningar kan du välja mellan olika typer av kryptering för ditt Wi-Fi. Vi rekommenderar de senaste standarderna: WPA2 eller WPA3. Läs manualen till din router för att få reda på hur du kommer åt och ändrar inställningarna.

I routrar från TP-Link ska du välja **Advanced** följt av **Wireless**.



24

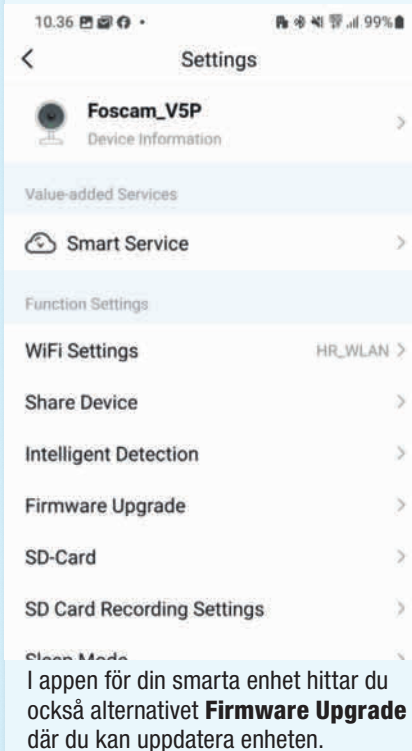
Stäng portarna i routern

Olika portar i din router gör att du kan komma åt enheter i ditt hem även när du inte är hemma. Om du inte använder den möjligheten bör du stänga portarna. I manualen till din router kan du läsa om hur du loggar in på routern och hittar listan över öppna portar.

26

Håll alla dina smarta enheter uppdaterade

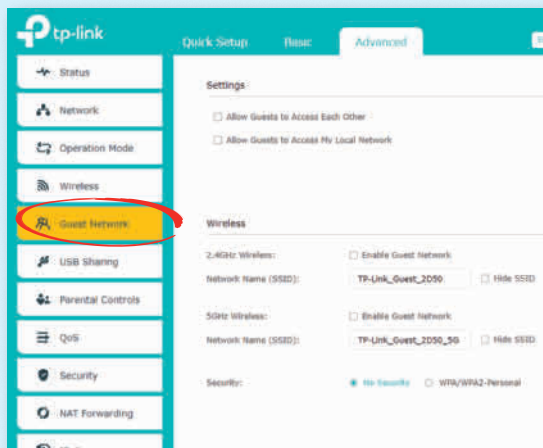
Smarta enheter som eluttag och kameror kan vara en säkerhetsrisk för alla enheter i ditt nätverk. Du kan undvika detta genom att hålla dina smarta enheter uppdaterade med hjälp av ny firmware. Du kan göra detta direkt från enheternas respektive appar.



25

Skapa ett separat nätverk för gäster

De flesta nyare routrar gör det möjligt att skapa ett extra trådlöst nätverk som du kan erbjuda dina gäster. Det här nätverket kommer inte åt andra enheter i nätverket, så ett gäst-nätverk är perfekt för att dela internetanslutningen. Läs manualen till din router för att ta reda på hur du ställer in ett gästnätverk på din router.

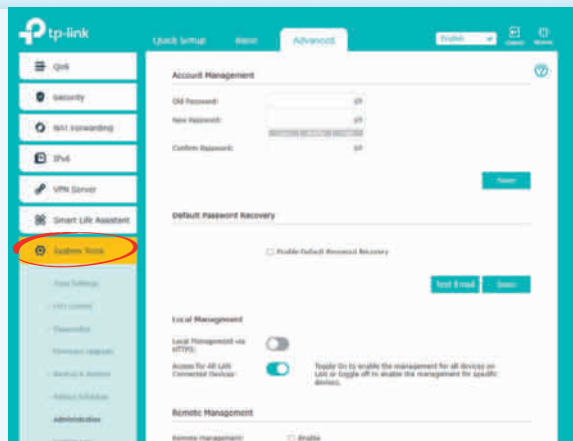


I TP-Links routrar ska du välja **Advanced** följt av **Guest Network**.

27

Stäng av routerns fjärråtkomst

Har du någonsin behövt komma åt din router när du inte är hemma? Inte? Då finns det inte någon anledning att funktionen ska vara aktiv, eftersom den kan vara en väg in i nätverket för hackare. Konsultera din routers manual för att ta reda på hur du stänger av den.

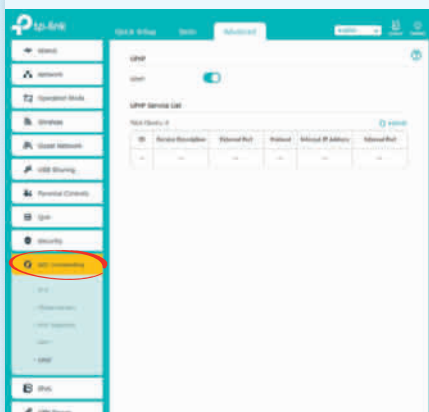


I routrar från TP-Link ska du gå via **Advanced** och **System Tools** för att stänga av fjärråtkomst.

28

Stäng av anslutning via UPnP i routern

Routerfunktionen UPnP, som du kan läsa mycket mer om på pctidningen.se/2513, skapades ursprungligen för att göra det enklare att ansluta olika enheter till varandra i nätverket. I praktiken har det dock sedan visat sig att funktionen också gjort det mycket enklare för kriminella att få ta sig in i nätverket. Därför rekommenderar vi att du letar upp UPnP i routerns manual, loggar in i routern och avaktiverar funktionen helt och hållet för att öka säkerheten.



UPnP-funktionen finns ofta i routerns meny för avancerade inställningar och NAT Forwarding.

32

Låt inte det trådlösa nätverket vara påslaget hela tiden

Om du bor nära andra människor kommer ni att kunna se varandras trådlösa nätverk. Även om ett oinbjudet besök i nätverket kräver att någon har gissat ditt lösenord, kan du minimera risken genom att stänga av routern helt på natten.

29

Se till att använda ett starkt Wi-Fi-lösenord

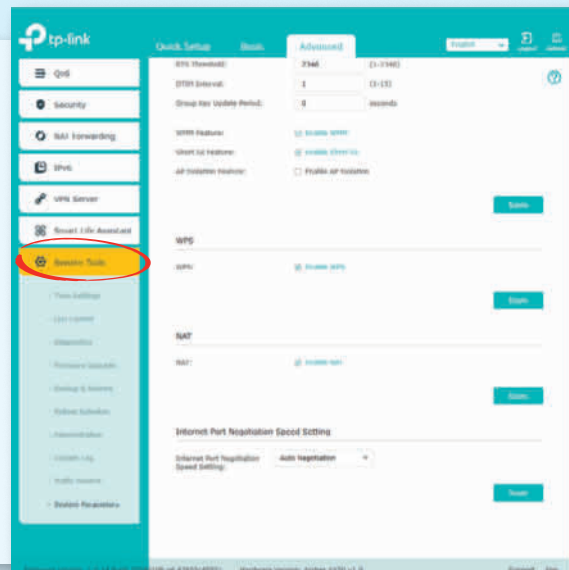
Om du använder enkla uttryck eller siffersträngar som lösenord för ditt trådlösa nätverk bjuder du i princip in obehöriga att ansluta till det. Det gäller också om du inte har ändrat tillverkarens standardlösenord som medföljde routern. Studera routerns bruksanvisning för att få reda på hur du ändrar koden för att logga in på det trådlösa nätverket.

31

Stäng av routerns WPS-funktion

WPS finns på din router och på trådlösa enheter som kan anslutas till nätverket. WPS gör att enheter kan anslutas enheter med en enkel knapptryckning, men kan också missbrukas, så stäng av den.

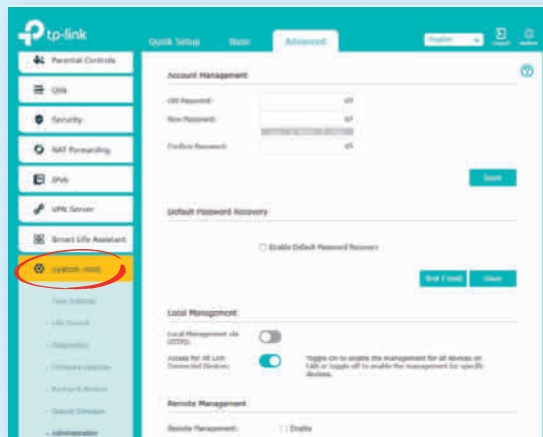
I routern har du möjlighet att avaktivera WPS-funktionen om du inte använder den.



33

Ändra lösenordet på routern

Du måste ange ett lösenord och ofta även ett användarnamn innan du kan ändra inställningar i routern, så det är viktigt att det är ett lösenord som du själv har valt. Följ de bästa och mest uppdaterade råden om säkra lösenord och byt sedan lösenord i routerns inställningar.



Du behöver som regel gå in i menyn **System** i routern för att byta ut standardlösenordet för inloggningen.

34

Byt ut logiska lösenord

Det är frestande att använda sig av lösenord som är lätta att komma ihåg eftersom vi lever i en tid då lösenord används för en mängd olika tjänster. Tyvärr finns det alltid människor med låg moral som försöker få tillgång till andras konton får lösenordet inte vara för lätt att gissa sig till, vare sig för människor eller avancerade program. Se därför till att undvika logiska siffersträngar eller vanliga ord. Läs mer om detta här:

pctidningen.se/2513

35



Looking for you...

Om din webbkamera har stöd för Windows Hello kan du logga in säkert med hjälp av ansiktsgenkänning.

Logga in med ett finger eller med ansiktet

Du kan minska antalet besvärliga lösenord som du måste memorera om du ersätter dem med biometri där det är möjligt. I Windows och på mobilen kan du välja ansiktsgenkänning eller fingeravtryck som alternativ till det klassiska lösenordet – och det är faktiskt säkrare än lösenord.

36

Gör dina lösenord extra långa

Ju längre ett lösenord är, desto längre tid tar det för en dator att knäcka det eller för en brottsling att gissa sig till det. Det är därför som de flesta säkerhetsexperten nu rekommenderar lösenord som består av 12 tecken eller fler.

37

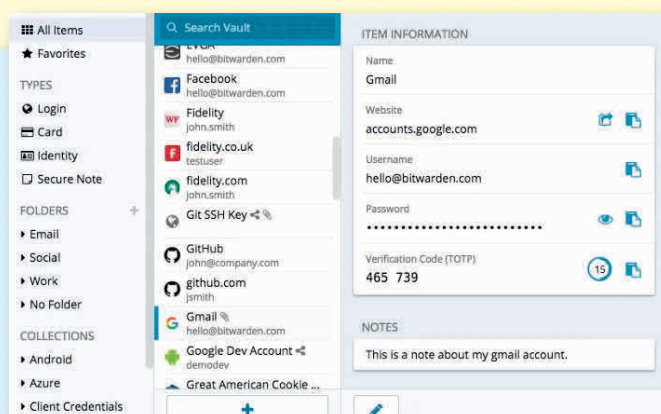
Hitta på rim och ramsor

Du kan göra din säkra och långa kod lättare att komma ihåg om du associerar den med något som betyder något för dig. Det kan vara ett rim eller en sång där du blandar specialtecken, siffror och versaler som sången Lit3tB0j@gsattavi11! eller sagan l1stug@b0dd3Petter.

39

Få hjälp att komma ihåg alla lösenord

Om du redan nu tycker att det är svårt att komma ihåg alla lösenord som du använder varje dag, blir det bara värre när de blir längre och mer komplicerade. Du kan lätta på den bördan genom att använda en lösenordshanterare. Det är ett fiffigt program som du öppnar med ett huvudlösenord, sedan håller programmet reda på alla de svåra enskilda lösenorden åt dig. Du kan till exempel använda programmet Bitwarden Free, som du hittar i vårt säkerhetspaket på pctidningen.se/2513.



Bitwarden Free är en utmärkt lösenordshanterare som kan hålla ordning på alla dina lösenord.

De mest uppenbara lösenorden är alldeles för lätta att gissa sig till, så undvik strängar av siffror och ord som du kan hitta i en vanlig ordbok.

38

Återanvänd aldrig dina lösenord

Även om det kan minska antalet lösenord att komma ihåg, bör du aldrig återanvända dina lösenord för olika tjänster. I värsta fall kan du ge brottslingar fri tillgång till alla tjänster där du har använt samma lösenord bara genom att snappa upp lösenordet för en av dem.

40

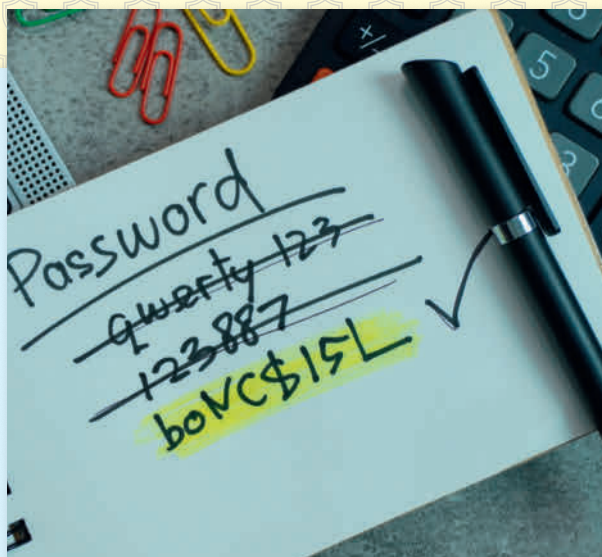
Har dina lösenord läckt ut på nätet?

Ibland inträffar stora dataläckor där hackare tömmer tjänster på information om deras registrerade användare. Ofta brottslingarna också tillgång till människors mejladresser och lösenord, vilket gör det riskabelt att använda samma inloggning på flera tjänster. Du kan kontrollera om din information har läckt ut genom att gå in i Chromes inställningar och välja **Integritet och säkerhet** följt av **Öppna säkerhetskontrollen**.

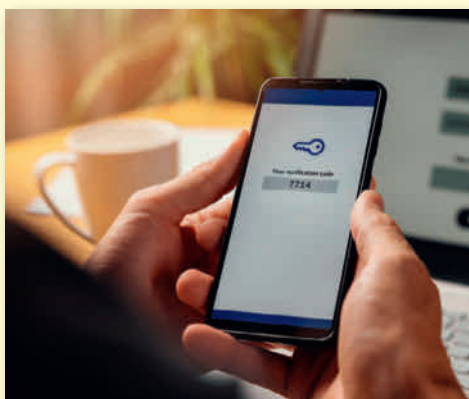
41

Skapa ett bra mixat lösenord

Receptet på ett bra och starkt lösenord har minst fyra säkra ingredienser: Det ska bestå av både stora och små bokstäver. De ska ha slumpmässiga placering. Kom ihåg att specialtecken som @, !, % och liknande inte är lätta att gissa sig till, samt slumpmässiga siffror. Läs mer här: pctidningen.se/2513



Skippa de logiska siffer- och bokstavssträngarna och skapa istället ett lösenord som verkar slumpmässigt.



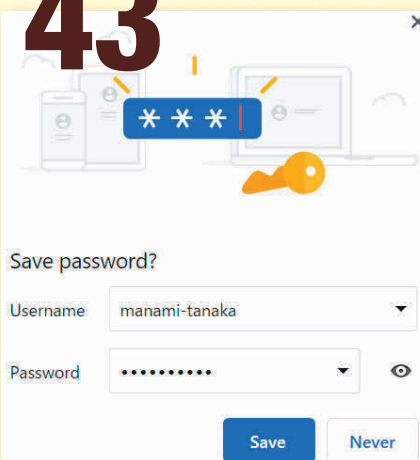
Med tvåstegsverifiering måste du också använda en slumpmässig engångskod.

42

Dubbelt skydd är mer effektivt

Det finns en anledning till att allt fler tjänster kräver att användare har tvåstegsverifiering med en app i mobilen där du autentiserar dig. Det är helt enkelt säkrare än en lösning som bara består av ett lösenord. Därför ska du se till att aktivera tvåstegsverifikation på alla tjänster och webbplatser där du har möjlighet att göra det.

43



Din webbläsare erbjuder sig gärna att spara lösenord till webbplatser åt dig, men det är inte helt riskfritt.

44

Hundens namn är inte tillräckligt säkert

Du kanske tror att främlingar aldrig kommer att kunna gissa ditt lösenord, även om du använt namnet på ditt husdjur eller ett barnbarn. När experter avråder från detta är det snarare för att namn och riktiga ord kan "gissas" genom ordboksuppslagningar som utförs av specialprogram.



Namn på husdjur är direkt dumt att använda som lösenord eftersom det gör dem alldeles för enkla att gissa.

Webbläsaren bör inte lagra dina lösenord

Det är frestande att säga ja när webbläsare som Chrome och Edge erbjuder sig att spara lösenordet för en webbplats, men det är inte lika säkert som att använda en riktig lösenordshanterare. Det beror på att dessa lösenord oftast är fritt tillgängliga för personer som lånar din dator och inte är särskilt väl skyddade mot hackare.



45

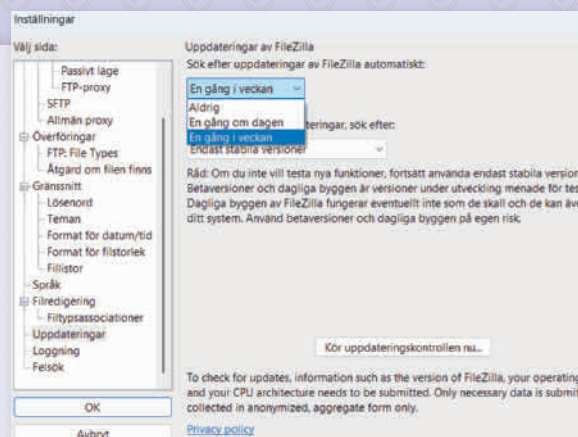
Undvik falska nedladdningssidor

Att använda en söktjänst för att hitta och ladda ner ett program på nätet är inte riskfritt. Du riskerar att hamna på en falsk nedladdningssida där du tror att du hämtar ett riktigt program men istället får ett virus i datorn. Därför bör du bara ladda ner program direkt från tillverkarens hemsida eller från pctidningen.se där vi hela tiden skannar allt efter virus.

46

Låt programmen uppdatera sig själva

Program som det var länge sedan du uppdaterade blir osäkra eftersom hackare haft gott om tid på sig att hitta säkerhetshål i dem. Det kan du undvika genom att hålla dina program uppdaterade. Många program kan till och med ställas in så att de på egen hand söker efter och installerar nya uppdateringar.



I **inställningarna** för de flesta program går det att aktivera automatisk uppdatering och till exempel låta programmet kontrollera en gång i veckan.



Här håller vi på att installera programmet doubleTwist när Delta Toolbar plötsligt dyker upp.

47

Undvik extra godis vid installationer

Du måste vara försiktig när du installerar program på din dator. Gratisprogram är särskilt pigga på att lägga till andra valfria program i installationen eftersom det ger utvecklaren lite extra inkomster. Läs därför noga vad du går med på under installationen och säg nej till det du inte känner igen.

48

Se vad dina program egentligen får göra

Vill du att ett tredjepartsprogram ska kunna se din position eller starta din webbkamera? Om inte ska du granska programmets behörigheter: Högerklicka på Start-knappen i Windows och välj **Inställningar**. Klicka sedan på **Sekretess och säkerhet**, välj en appbehörighet – till exempel **Kamera** – för att se vilka program som får använda din webbkamera.

49

Avinstallera alla överflödiga program

Om du har haft din dator länge har du troligtvis installerat en hel del program under årens lopp som nu ligger på datorn – även sådana du inte längre använder. De tar inte bara upp onödig plats, de kan vara en säkerhetsrisk. Se därför över inställningarna och ta bort onödiga program. Läs mer om detta här: pctidningen.se/2513

50

Körs det ransomware på datorn?

Om datorn känns slö kan det bero på skadliga program som arbetar i det fördolda. Till exempel tar de fruktade utpressningsprogrammen upp mycket plats på hårddisken eftersom de låser dina filer och kräver en lösensumma. Kontrollera detta i Aktivitetshanteraren genom att klicka på **Ctrl + Shift + Esc** och titta i kolumnen **Disk**.

kerhed och anonymitet

andelser

Placering

Kamera

Mikrofon

Stemmeaktivering

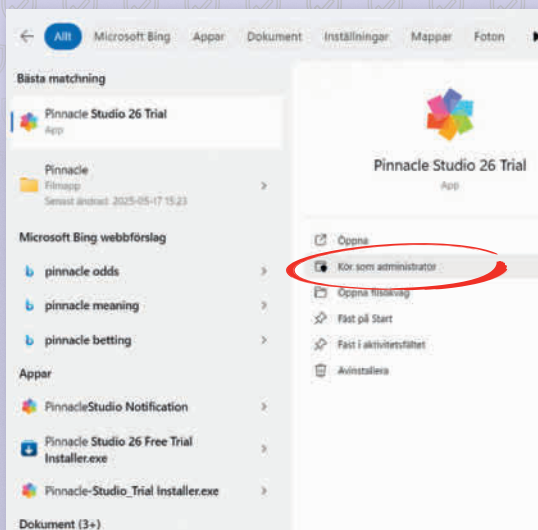
Meddelelser

I Windows inställningar under kategorin **Sekretess och säkerhet** kan du se vilka behörigheter dina program har.

51

Får dina program några uppdateringar?

Även bra program överges förr eller senare av tillverkaren och uppdateringar slutar att komma. Det innebär att du inte kan täppa till säkerhetshål vilket i sin tur gör det riskabelt att fortsätta använda det övergivna programmet. Därför bör du undersöka när dina program senast uppdaterades.



Sökresultaten i Start-menyn gör att du kan köra program som administratör.

52

Ge inte obegränsad tillgång till datorn

När du bläddrar bland dina program i startmenyn eller högerklickar på en genväg har du möjlighet att köra program med administratörsrättigheter. Det bör du enbart göra om ett program kräver det för att fungera. Med administratörsåtkomst får programmen mycket mer makt över datorn.

53

Ge filerna en extra kontroll

Du kan inte alltid villkorslöst lita på ditt antivirusprogram när det godkänner ett program eller en fil. Om du vill vara helt säker bör du rådfråga en oberoende tredje part. Vi rekommenderar hemsidan [virustotal.com](https://www.virustotal.com) där du kan ladda upp filer och få reda på hur de bedöms av alla ledande säkerhetsprogram på marknaden.



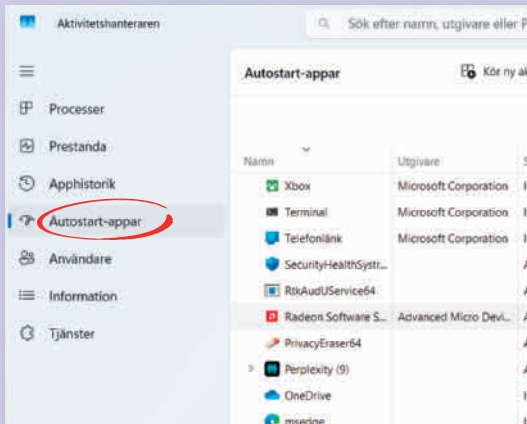
På VirusTotal klickar du bara på **Choose file**, väljer en fil på din hårddisk, och får svar på om filen är farlig.

DVD Shrink är ett bra program för att spara DVD-filmer på hårddisken, men det fick sin senaste uppdatering 2004 och är därför osäkert att använda.

54

Granska vilka appar som autostartar

Alla program som automatiskt med Windows är inte bara en belastning på datorns resurser. Även skadliga program kan gömma sig där för att starta varje gång du startar datorn. Ta därför en kritisk titt under fliken **Autostart-appar** i Aktivitetshanteraren, som du öppnar med **Ctrl + Shift + Esc**.



Under **Autostart-appar** kan du se vilka program som startar med Windows.

55

Ge program begränsad tillgång till datorn

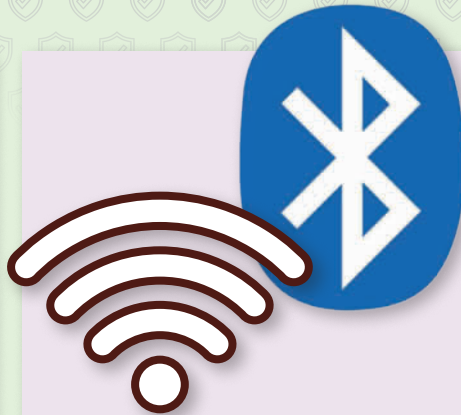
Ransomware är en typ av virus som först krypterar dina filer och sedan kräver dig på pengar för att låsa upp dem. Men om viruset inte har tillgång till dina filer kan det inte kryptera dem. Läs därför mapparna med **Kontrollerad mappåtkomst** i inställningarna för Windows inbyggda säkerhetsfunktion **Windows-säkerhet**.



56

Installera antivirus

Om du använder en iPhone är du redan väl skyddad, men om du har en Android-mobil är det en bra idé att skydda dig med ett antivirus-program – precis som du gör på din dator. Sophos Intercept X for Mobile är bästa gratis antivirus-appen för Android och på vår webbplats visar vi hur du använder den. Du hittar artikeln via den här adressen: pctidningen.se/2513



Det finns ingen anledning att ha Wi-Fi eller Bluetooth påslaget när du inte använder trådlösa anslutningar.

57

Stäng av Bluetooth och Wi-Fi

Wi-Fi och Bluetooth är bra trådlösa anslutningar, men kan vara en väg in för hackare. Du bör bara ha Wi-Fi påslaget när du använder betrodda nätverk. Bluetooth ska bara vara aktiverat när du behöver använda ett trådlöst headset eller högtalare. När du inte använder anslutningarna kan du stänga av dem tillfälligt i inställningarna.

58

Håll mobilen uppdaterad

Säkerhetshål i mobilens programvara brukar dyka upp med jämna mellanrum och hackare står i kö för att utnyttja dem, så se till att operativsystemet i din mobil alltid är uppdaterat. Kontrollera om det finns en uppdatering genom att öppna inställningarna för din iPhone eller Android-mobil och gå till den kategori som handlar om programuppdateringar eller information om din mobil.

< **Programvaruuppdatering****Programvaran är uppdaterad.****Uppdatera information**

- One UI-version: 7.0
- Android-version: 15
- Aktuell version: S921BXXU5BYD9 / S921BOXM5BYD9 / S921BXXU5BYD9
- Säkerhetskorrigeringsnivå: 1 april 2025

I mobilens inställningar kan du tydligt se om enheten är uppdaterad.

59

Välj ett bra lösenord för din hotspot

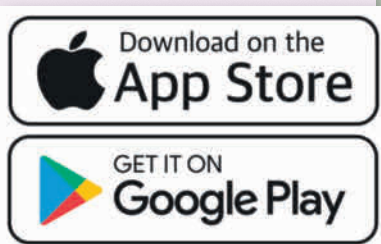
Du kan dela din mobil data och komma åt webben med en annan enhet via mobilens internetdelning. Det kallas för mobil hotspot. Om du gör det måste du skydda din hotspot med ett bra lösenord. Du ändrar lösenordet i inställningarna, där du också aktiverar din hotspot. Kom ihåg att använda stora och små bokstäver, specialtecken och siffror i lösenordet.

60

Hämta bara appar från officiella butiker

Det enklaste sättet för hackare att ta sig in i din mobil är via appar som innehåller skadlig programkod. Det kan leda till att dina inloggningsuppgifter stjäls, blir överöst av reklam, eller att du blir övervakad. Om du hämtar appar från officiella appbutiker minimerar du den risken.

På iPhone ska du hämta appar från App Store. På Android ska du använda Play Butik.



61

Om du inte håller dina appar uppdaterade blir det enklare att infektera dem med malware.

**Uppdatera dina appar**

Precis som du måste hålla mobilens operativsystem uppdaterat för att stärka säkerheten, måste du komma ihåg att uppdatera mobilens appar regelbundet. Läs mer om hur du uppdaterar appar på adressen pctidningen.se/uppdatera-appar

62

Säkerhetskopiera dina bilder

Numera lagrar de flesta av oss foton på våra mobiler, eftersom vi tar våra foton på våra mobiler. Men om något händer med din mobil kan du riskera att förlora dina foton om du inte har sparat dem någon annanstans också. Det är därför du bör säkerhetskopiera dina foton då och då. Läs hur du bäst gör det här: pctidningen.se/2513

[Postens information]: Din försändelse har anlänt till utlämningsstället, men den kan inte levereras eftersom informationen om förpackningen är oklar.

Vänligen klicka på länken nu: <http://is.gd/ByequFC?psq=olbjgei>

Vi skickar igen så snart informationen har uppdaterats.

Ett typiskt bluffmeddelande med en länk som du uppmanas att använda.

63

Se upp för svindleri i din sms-inkorg

Precis som i din inkorg för mejl kan du att få bedrägerier via SMS. Det kan vara ett sms om en misslyckad leverans av ett paket som i skärmbilden här. Det kan också vara falska meddelanden från låtsas att de kommer från myndigheter, eller meddelanden om att du har vunnit ett pris.

64



Undvik offentliga USB-portar

Om du stöter på en publik USB-laddningsstation kan det vara frestande att koppla in din mobil, men du bör vara försiktig. Hackare kan använda USB-kontakter för att installera skadlig kod på din mobil. Metoden kallas "juice jacking" och är utformad för att stjäla din information.

66

Lås mobilen med biometri

Biometri i mobilen, som fingeravtryck eller ansiktigenkänning, gör att du snabbt kan låsa upp din mobil utan att använda ett lösenord. Det är också ett säkert sätt att skydda information, eftersom det krävs dina unika fysiska egenskaper för att låsa upp mobilen.



I säkerhetsinställningarna kan du aktivera de biometriska funktioner som mobilen har.

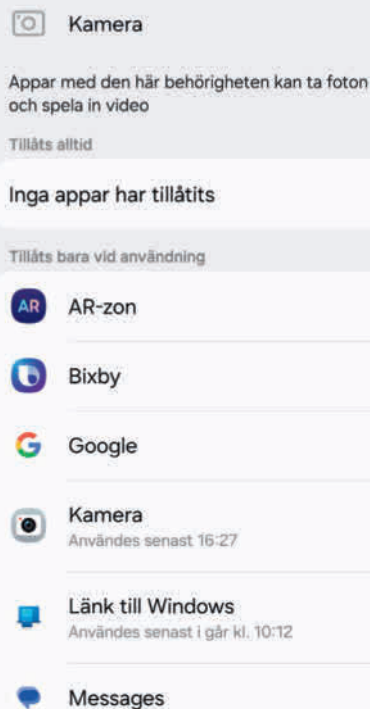
65

Kontrollera dina apparers behörigheter

Du bör undersöka vilka appar som har tillgång till mobilens funktioner. På en Samsung-mobil hittar du listan över behörigheter i **Appar**, där du ska trycka på de ter punkterna högst upp till höger och välja **Behörighetshanterare**. Metoden kan variera något på andra mobiler, men vanligtvis måste du gå in i inställningarna för appar för att hitta översikten där du enkelt kan inaktivera de oönskade behörigheterna.

Du ska vara särskilt när det handlar om behörigheter för mikrofon, GPS, kamera, samtal och SMS.

Det ska inte finnas några appar som alltid har behörighet att använda mobilkameran. Om du ser det ska du ta bort behörigheten.





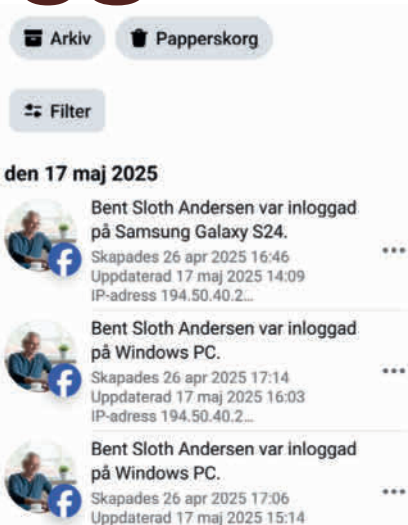
67

Gör din profil privat

För att göra din profil privat och på så sätt minimera risken för identitetsstöld, klickar du på din profilbild i det övre högra hörnet på Facebook och väljer **Inställningar och integritet**. Välj **Integritetskontroll** och genomför de olika guiderna på sidan.

Du bör se till att det bara är du och dina vänner som kan se din information på Facebook.

68



Om du ser en enhet som du inte känner igen klickar du på de tre prickarna bredvid enheten och väljer **Logga ut**.

Kontrollera var du är inloggad

Om du har en misstanke om att någon annan har tillgång till din profil, kan du ta reda på det. Klicka på din profilbild uppe i det högra hörnet och välj **Inställningar och integritet**. Klicka **Aktivitetslogg** följt av **Där du är inloggad**. Där ser du överallt där du är inloggad.

69

Se upp för bedrägerier och falskt innehåll

Facebook har övergett all fakta-kontroll, vilket lett till att tjänsten är full av falskt innehåll. Tyvärr är det inte bara osant, det kan också vara direkt farligt att klicka på det. En länk till en falsk artikel kan till exempel leda till en bluffsajt där du blir bestulen på känslig information eller riskerar att installera ett virus. Var extra kritisk mot alla inlägg och information på Facebook.

70

Kom ihåg att logga ut

Det kan låta trivialt, men du måste komma ihåg att logga ut från Facebook när du inte använder tjänsten. Det gäller i synnerhet om du varit inloggad på en offentlig dator eller en dator som du delar med andra, annars riskerar du att obehöriga får tillgång till din profil.

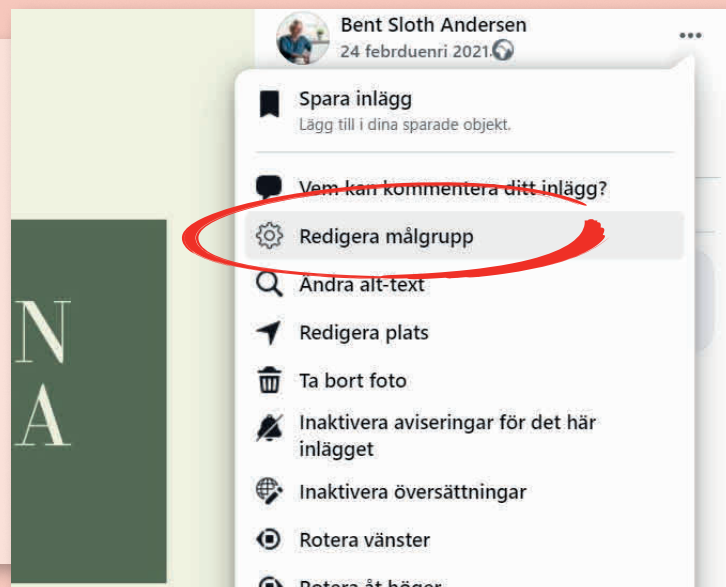
När du är utloggad, kontrollera att webbläsaren inte har sparat din mejladress och ditt lösenord. Om den gjort det, se till att ta bort det.

71

Gör profilbilden privat

Bedragare älskar att använda Facebook för att stjäla offers identiteten och sedan använda den för att lura andra. Många Facebook-profiler har fri tillgång till profilbilder som bedragare enkelt kan stjäla och missbruka. Du kan förhindra det genom att göra din profilbild privat så att bara du och dina vänner kan öppna den. Andra besökare kan fortfarande se bilden, men bara i miniatyrformat, vilket inte är till någon större nytta för hackare.

Klicka på din profilbild, på **Visa profilbild** och på de tre punkterna. Välj **Redigera målgrupp**. Välj **Vänner**.

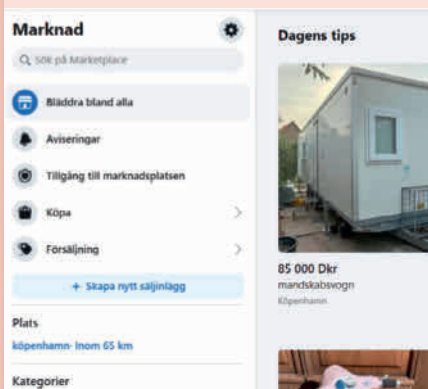


72

Var försiktig på marketplace

Marketplace är Facebooks marknadsplats där du kan köpa och sälja begagnade varor. Det finns dock många exempel på att både köpare och säljare har blivit lurade.

Säljare kan erbjuda Apple-produkter eller märkeskläder till onaturligt låga priser, men i själva verket sälja en piratkopia eller ingenting alls. Ett annat exempel är köpare som betalar via oseriösa tjänster där du inte kommer att se ett spår av dina pengar. Dessutom riskerar du att köpa stöldgoods.



På Facebook Marketplace måste du vara extremt kritisk när du handlar.

73

Se upp med länkar i Messenger



Om du får ett meddelande på Facebooks chattjänst Messenger som uppmanar dig att klicka på en länk bör du vara skeptisk. Det gäller framför allt om det kommer från en främling, men även om det är en av dina Facebook-vänner som är avsändare. Det kan vara bedragare i farten som har hackat din väns profil.

Då bör du kontakta din vän via andra kanaler än Messenger för att se om det är han eller hon skickat meddelandet med länken eller inte.

74

Tänk på vad du delar

Facebook är utformat för att du ska kunna dela med dig av dina upplevelser och intryck till vänner och familj, men tänk på vad du faktiskt delar med dig av till andra.

Om du inte har en privat profil kan i princip vem som helst se vad du delar med dig av och använda din information mot dig. Det gäller inte bara vad du skriver i status-uppdateringar, utan också i stor utsträckning vad som skrivs om dig på din profil. Överväg att dölja din privata information. Läs hur du gör det här: pctidningen.se/2513

75

Aktivera varningar

I Facebooks inställningar kan du aktivera en funktion som kommer att meddela dig om någon loggar in på ditt konto från en ovanlig plats. Då kan du reagera snabbt och först se till att logga ut dem igen. Därefter bör du byta lösenord direkt och även aktivera tvåstegsverifikation för att logga in.

Kontrollera dina varningar

Prata om hur vi kan meddela dig om någon loggar in på ditt konto från en plats vi inte känner igen. Vi kommer att meddela dig vilken enhet som användes och var den är tillgänglig.

Facebook

Vi skickar en Facebook-notifiering till dig.



E-post

Vi skickar en avisering till renix@adshome.dk



Funktionen finns i sekretessinställningarna genom att klicka på **Sekretesskontroll** och sedan välja **Så skyddar du ditt konto**.

76

Bli bara vän med personer du känner

Om du får en vänförfrågan från någon du inte känner eller inte har träffat, då bör du vänta med att acceptera förfrågan. Speciellt om du inte har några gemensamma vänner med personen. I dessa fall kan det vara en bedragare. Läs om hur du upptäcker en falsk profil här: pctidningen.se/2513

Lösenord och säkerhet

Inloggning och återställning

Hantera lösenord, inställningar för inloggning och återställningsmetoder.

Byt lösenord

Tvåfaktorsautentisering

Sparad inloggning

I **inställningarna för sekretesskontroll** kan du byta lösenord och aktivera tvåstegsverifikation.

77

Se till att använda tvåstegsverifikation

Tvåstegsverifikation kräver att du anger en kod från din mobil utöver ditt lösenord när du loggar in. Det gör det svårt för hackare att komma åt ditt konto eftersom de även behöver till din mobil. Du aktiverar funktionen i säkerhetsinställningarna.

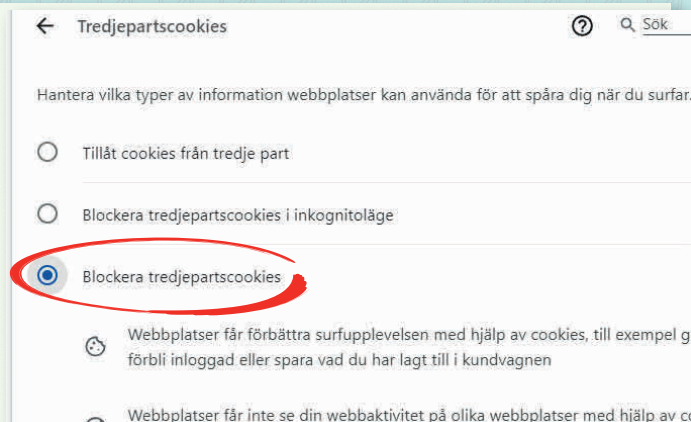


78

Rensa bort snokande cookies

Cookies kan spara dina inställningar så att webbplatser du besöker ofta laddas snabbare, men cookies kan också användas för att spåra dig mellan olika webbplatser. Du bör vara särskilt uppmärksam på så kallade tredjeparts-cookies, eftersom dessa cookies sätts av någon annan än den webbplats du besöker.

Dessa tredjepartscookies kommer vanligtvis från olika reklamföretag som spårar dig och vad du gör på nätet för att sedan kunna överösa dig med annonser som är riktade till dig baserat på vad du gör på nätet. Det betyder att de annonser som du ser på webbplatser kommer att relatera till vad du tidigare har gjort på nätet, vilket kan kännas integritetskränkande.



I Google Chrome och de flesta andra webbläsare kan du stoppa spårning av cookies från tredje part. I Chromes gör du det under **Integritet och säkerhet**-inställningarna.

79

Granska behörigheter

Många webbplatser vill gärna ha tillgång till olika delar av din dator, till exempel kameran, mikrofonen och datorns position, medan andra webbplatser vill kunna skicka meddelanden till dig via webbläsaren. Du bör regelbundet granska och vid behov justera dessa behörigheter så att du inte ger webbplatser onödiga friheter.

Behörigheter



Plats

Webbplatser får fråga efter din plats



Kamera

Webbplatser får begära åtkomst till kameran



Mikrofon

Webbplatser får begära åtkomst till mikrofonen

I Chrome kan du kontrollera behörigheter genom att öppna **Integritet och säkerhet**-inställningarna och klicka på **Webbplats-inställningar**. Där kan du se behörigheter och vilka webbplatser som har godkänts.

80

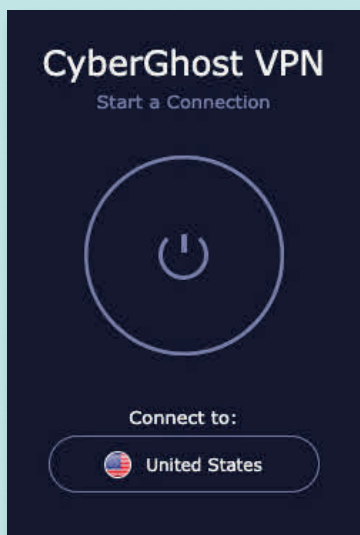
Stäng webbläsaren med jämna mellanrum

Att ha webbläsaren igång flera dagar i sträck belastar datorn och kan medföra säkerhetsrisker. När du stänger webbläsaren raderas vissa temporära filer och sessions-cookies som annars skulle kunna användas för att övervaka dig. Gör det därför till en vana att stänga webbläsaren varje dag.

81

Ta bort lagrade lösenord

Att låta webbläsaren komma ihåg dina lösenord kan verka bekvämt, men det innebär en säkerhetsrisk. Om din dator eller ditt Google-konto – om du använder Chrome som webbläsare – utsätts för ett intrång kan obehöriga komma åt alla dina sparade inloggningar. På vår webbplats visar vi hur du tar bort sparade lösenord från både Chrome och webbläsaren Edge: [pctidningen.se/2513](https://www.pctidningen.se/2513)



82

Använd en VPN-tjänst

VPN krypterar din internetanslutning och döljer din IP-adress. Det gör det svårare för webbplatser och hackare att övervaka dig. De flesta VPN-tjänster kostar pengar, men du kan installera tillägget CyberGhost VPN Free Proxy utan att betala. Läs mer om hur du använder det här: [pctidningen.se/2513](https://www.pctidningen.se/2513)

Med kostandsfria webbläsartillägget CyberGhost VPN Free Proxy får du en utmärkt VPN till Chrome och Firefox, så att du kan dölja din IP-adress.

83

Klicka inte på reklam

Annonser på internet kan vara mer än bara irriterande. Vissa annonser är utformade att ta dig till skadliga webbplatser eller installera skadlig programkod på din dator. Dessa annonser försöker få dig att klicka på dem med falska varningar eller erbjudanden om billiga produkter eller hjälpsamma datorprogram.

Även till synes fullt legitima annonser kan vara bedrägliga, så du bör undvika att klicka på dem om du inte är helt säker på vem som står bakom dem.

84

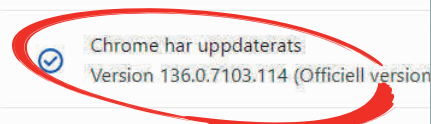
Se upp med vad du hämtar från internet

Många säkerhetsproblem börjar med en obetänksam nedladdning från webben. Undvik att ladda ner filer från okända eller opålitliga källor. Om du är osäker, använd alltid ditt antivirusprogram för att undersöka de hämtade filerna.

Var särskilt uppmärksam på webbplatser som erbjuder gratisversioner av annars dyra program. Kom ihåg att om något verkar för bra för att vara sant, så är det förmodligen det.



Google Chrome



Få hjälp med Chrome

Rapportera ett problem

Integritetspolicy

Om du använder Chrome kan du se om webbläsaren är uppdaterad i **Om Chrome**-kategorin i inställningarna.

85

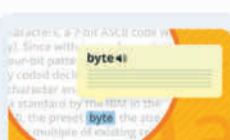
Håll webbläsaren uppdaterad

Gamla versioner av webbläsare, liksom annan programvara, har ofta säkerhetshål som hackare kan försöka utnyttja.

Säkerhetshålen täpps till när webbläsaren uppdateras. De flesta webbläsare – som Google Chrome och Microsoft Edge – uppdateras automatiskt, men det krävs att du manuellt startar om webbläsaren genom att stänga ner den och öppna den igen.



WPS PDF - Read, Edit, Fill,...



Shazam: Find song names...



86

Undersök tilläggen grundligt

Webbläsartillägg kan göra mycket gott, men de kan också vara väldigt skadliga. Kontrollera vilka tillägg du har installerat och ta bort de som inte används. Titta på omdömen och kontrollera utgivarens trovärdighet. Läs hur du tar bort tillägg här: pctidningen.se/2513

87

Ha en säker webbläsare

Vissa webbläsare, som Firefox och Brave, fokuserar på integritet och säkerhet, och ger standard mer kontroll över vad som delas med tredje part. Brave kan blockera spårningscookies och annonser automatiskt, medan Firefox har avancerade alternativ för att hantera sekretess. Båda finns här: pctidningen.se/2513



Brave och Firefox är bra på att skydda ditt privatliv när du är ute på nätet.

88

Var uppmärksam på domänbluffar

Nätfiske utförs ofta via domäner som liknar som kända webbplatser men med små skillnader, som "facebook.com" istället för "facebook.com". Kontrollera alltid domänen noga innan du loggar in eller laddar ner något. Ett enda besök på fel webbplats kan ge en hackare tillgång till din information.



89

Titta efter märkningen

Trygg E-handel är en certifiering som ges till nätbutiker som uppfyller ett antal krav på säkerhet, transparens och konsumentskydd. När du handlar hos en sådan butik har du en extra garanti för att dina rättigheter respekteras. Du har också tillgång till kostnadsfri juridisk hjälp vid eventuella tvister. Så se till att titta efter märkningen, särskilt när du handlar på nya sajter.



Märkningen ser ut såhär, och du hittar den vanligtvis längst ner eller högst upp på butikens hemsida.

90

Undvik publika datorer

Allmänna datorer, till exempel på bibliotek eller hotell, är riskabla. När du handlar på nätet anger du ofta känslig information som betalinformation och adresser du inte vill att andra ska få tillgång till. Använd alltid din egen dator när du handlar på nätet, se till att den är uppdaterad och att den har ett antivirusprogram installerat.

91

Läs igenom villkor och bestämmelser noggrant

Många klickar på "acceptera" utan att läsa igenom villkoren, men de innehåller viktig information om exempelvis returpolicy, leveranstider och avgifter. Särskilt vid köp från utlandet kan det tillkomma extra kostnader eller finnas ett sämre konsumentskydd. Ta dig tid att läsa igenom villkoren så att du vet vad du går med på.

92

Kontrollera butikens fysiska adress

En pålitlig webbutik uppger alltid sin fysiska adress, även om den bara säljer på internet. Om adress saknas eller den ser mystisk ut bör du vara försiktig. Använd Google Maps för att kontrollera om den finns och matchar företagets profil. Många bluffbutiker har påhittade adresser eller hänvisar till servicekontor, så ta det som en varning.

93

Betala med Swish

Swish är en snabb, smidig och säker betalmetod när du handlar på nätet. Dina kortuppgifter delas inte med butiken när du använder Swish, och eftersom du godkänner betalningen via mobilen får du bättre kontroll över de betalningar du har gjort. Transaktionerna visas dessutom tydligt både i appen och hos banken, så du har tillgång till dokumentation om det skulle uppstå problem. Använd därför Swish när det är möjligt.

94

Kontrollera företagets organisationsnummer

Ett effektivt sätt att kontrollera om du har att göra med en äkta butik är att kontrollera organisationsnumret, som du ska hitta på butikens webbplats. Det är företagets officiella registrering i Sverige. På bolagsverket.se kan du se om företaget existerar och vem som står bakom företaget. Om organisationsnummer saknas eller är falskt är det vanligtvis ett tecken på bedrägeri.

©2024 Elgiganten AB. All rights reserved.
Organisationsnummer: 556471-4474

[Köpvillkor](#)[Produktkategorier](#)[Varumärken](#)[Cookieinställningar](#)

Nätbutiken visar sitt organisationsnummer antingen på startsidan eller på kontaktsidan.



Med Swish får inte butiken ditt kortnummer, så om butiken blir hackad är dina pengar fortfarande i säkerhet.

95

Handla bara från webbplatser med https

Om det står "https" och det finns ett hänglås i adressfältet betyder det att förbindelsen mellan dig och nätbutiken är krypterad. Det skyddar din information från att fångas upp av tredje part. Om webbplatsen bara använder "http" bör du undvika att ange personuppgifter, särskilt kreditkortsinformation. Idag markerar de flesta webbläsare webbplatser utan en säker anslutning som "Inte säker".



https://www

97

Se upp när du handlar med privatpersoner

När du handlar med privatpersoner har du inte samma konsument-skydd som när du handlar från en nätbutik. Betala aldrig i förskott om du inte litar fullt ut på säljaren. Träffa motparten personligen och betala först när du fått varan. Om varan ska skickas bör du använda säkra betalösningar och se till att använda spårning av försändelsen.

99

Spara orderbekräftelsen

Spara alltid orderbekräftelsen när du har gjort ett köp. Den kommer ofta antingen som mejl eller PDF och fungerar som dokumentation på vad du köpt, när och till vilket pris. Den är användbar vid returer och reklamationer eller om varan aldrig dyker upp. Se till att spara orderbekräftelsen på ett säkert ställe så att du alltid kan hitta den.

98

Granska ditt bankkonto efter köpet

Efter köp på nätet är det en god vana att kontrollera dina banktransaktioner. Se till att det belopp du godkänt stämmer överens med det som betalats ut. Obehöriga eller dubbla uttag kan vara ett tecken på fel eller missbruk. Om du märker något misstänkt ska du genast kontakta din bank. Ju tidigare du reagerar, desto bättre.

Order confirmation

Hi martinlorentsen77 user,

Thank you for shopping with us. Your order **3035585457205239** is confirmed. We'll let you know when your order ships.

[View your order](#)

Order details

Placed on May 23, 2024, 04:58

Med en orderbekräftelse kan du enkelt dokumentera vad du köpt och vad det kostade ifall du behöver det.

96

Kolla alltid omdömen

Användaromdömen på Trustpilot kan ge dig en uppfattning om hur företaget behandlar sina kunder. Titta både på betyget och på kommentarerna. Kolla särskilt upp de dåliga recensionerna. Om andra har haft problem med leverans, kundtjänst eller returer bör du vara extra försiktig.

Hitta ett företag du kan lita på

Riktiga omdömen skrivna av riktiga människor.

Sök efter företag eller kategori

Sök efter butiken på Trustpilot och läs omdömen noga.

100

Kontrollera avsändaren

Det är inte alltid tydligt varifrån det du köper på nätet skickas. Nätbutiker kan ha svenskt namn och en svensk domän men skickar från Kina eller andra länder utanför EU. Det kan leda till långa leveranstider, högre fraktkostnader samt risk för tull och moms. Kontrollera alltid leveransinformationen i köpvillkoren innan du beställer. De står i det finstilta, men kan ha stor inverkan på dina kostnader.



Det kan bli dyrt om vara du köper på nätet skickas från en plats utanför EU.