

Internetguide #38



Kom igång med säkrare mobiltelefon!



Anders Thoresson

I den här guiden lär du dig...

- ☒ Om säkerhetsproblem och annat som påverkar din integritet när du använder en mobiltelefon.
- ☒ Generella beskrivningar av de problem som finns.
- ☒ Tips om inställningar för Iphone, Android och Windows Phone.

Innehåll

Inledning 4

Det kan mobilen avslöja 6

Det kan mobilen avslöja	7
En telefon utan pinkod	7
Spara inte känsliga kontakter i adressboken	7
Rensa i historiken	8
Se upp med trådlösa nätverk	8
Telefonen letar efter kända nätverk	8
Stäng av Bluetooth	9
Kryptera telefonsamtalen	9
Kryptera datakommunikationen	10
Kryptera nättrafiken	10
Kryptera e-posten	12
Välj webb före app	12
Fabriksåterställning raderar inte alla data	13
Malware stjälar information	13
Försiktigt med molntjänsterna	13
Mobilnätet vet var telefonen är	14
IP-adresser ger ungefärlig plats	14
Insamling av MAC-adresser	14
Positionering med gps	15
Skydda röstbrevlådan med en pinkod	15

Inställningar för din telefon 16

iPhone	17
Android	28
Windows Phone	38

Lär dig mer 46

Lär dig digitalt självförsvar!	47
--------------------------------	----

Inledning

En smartphone är ett fantastiskt verktyg. Men är du oförsiktig kan den också avslöja mer om dig och vad du gör än du tänkt dig.

Det du kan och bör göra är att förstå vilka problemen är och i vilka situationer de uppstår. På så sätt kan du i möjligaste mån fatta aktiva beslut om vad du ska göra för att undvika, eller i alla fall minimera integritetsproblemen. I den här guiden får du generella råd och steg-för-steg-instruktioner som visar dig rätt i telefonens menyer.

Men några hundra procentiga garantier för att telefonen därmed har blivit säker går inte att ge. Man kan bara säga att den har blivit säkrare. Ett säkerhetshål som är okänt idag kan få stor spridning i morgon. Dessutom finns risken att telefontillverkare och operatörer samlar in information från telefonerna på ett sätt som vi användare inte känner till eller saknar möjlighet att skydda oss mot.

I en Iphone finns en funktion som heter *Vanliga platser*. Den samlar in information om var telefonen brukar befinna sig och visar det i en kartbild.

Apple säger att informationen aldrig lämnar telefonen, utan samlas in för att förbättra personanpassade tjänster. I Android telefoner finns en liknande funktion, där under namnet Platshistorik. Skillnaden jämfört med Apples lösning är att informationen synkroniseras med Googles nättjänster och bland annat görs tillgänglig för användaren på <https://maps.google.com/locationhistory>.

Bland Edward Snowdens avslöjanden har det funnits mycket som handlar om mobiltelefoner och mobilnät. Sensommaren 2015 visade Dagens Nyheter i en serie artiklar¹ vilken detaljerad information som mobiloperatörerna är skyldiga att spara om sina användare, enligt datalagringsdirektivet.

Eftersom teknikutvecklingen går snabbt innebär det att det inte går att säga något om vilka problem som kan dyka upp i framtiden, eller om säkerhetsproblem som idag är svåra att utnyttja kan bli mer lättillgängliga längre fram.

Tips! Använd mobilen för att skydda dina inloggningar.

Lättgissade lösenord och inloggningsuppgifter som har kommit på drift är ett problem för alla som lever i en uppkopplad värld där vi lagrar allt mer av vår information i olika molntjänster.

Ett enkelt sätt att minska riskerna är att använda så kallad tvåstegsinloggning där det är möjligt. Sannolikt använder du redan tvåstegsinloggning idag, utan att vara medveten om det:

Ska du göra bankärenden räcker det inte med ett vanligt lösenord. Du behöver också mata in en engångskod från bankdosa eller på något annat sätt komplettera ditt lösenord. Anledningen är att ett användarnamn och lösenord lätt kan komma på drift, men att det är svårare för någon att dessutom komma över din bankdosa.

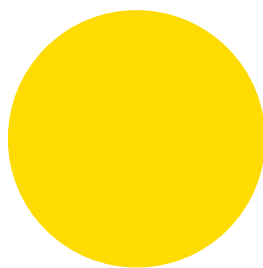
Lösenordet är den ena "faktorn", engångskoden från bankdosa den andra.

Molntjänster har däremot sällan möjlighet att skicka ut egna dosor. I stället används ofta mobiltelefonen. Antingen behöver användaren installera en speciell app som genererar engångskoder eller också skickas de via sms.

En lista med tjänster där det är möjligt att aktivera tvåstegsinloggning finns på <https://twofactorauth.org/>.



**Det kan
mobilen
avslöja**



Det kan mobilen avslöja

I värsta fall kan din smarta telefon avslöja:

- Vem det är du kommunicerar med.
- Innehållet i kommunikationen.
- Var du befinner dig, eller var du har befunnit dig.

Använd inte ett nummer kopplat till dig

Inkommande och utgående samtal lagras i samtalsloggar hos operatören. Om du någon gång vill ringa ett anonymt samtal, använd då inte ett telefonnummer som går att koppla till dig.

En telefon utan pinkod

Utan knapplåset aktiverat kan den som hittar din telefon se vilka kontakter som finns i adressboken, läsa e-post, använda de webb-tjänster du är inloggad på och så vidare. Aktivera telefonens lösenord så att den inte går att använda utan rätt kod. Det minskar risken för att någon som hittar en glömd telefon i taxin kommer åt känslig information.

Men tyvärr är varken lösenordet eller pinkoden någon garanti för att informationen i telefonen är säker. Både Iphone och olika Android-modeller har haft buggar som gjort det möjligt att helt eller delvis ta sig förbi lösenordet genom att trycka på olika knappar i en viss sekvens.

Vissa telefonmodeller har inställningar som raderar allt innehåll efter ett visst antal misslyckade försök att låsa upp den. Det är inte säkert att innehållet raderas på ett sådant sätt att det inte går att återskapa, men med funktionen aktiverad försvårar man åtminstone något för den som eventuellt kommer över telefonen.

Spara inte känsliga kontakter i adressboken

Telefonnummer och andra kontaktuppgifter till personer som du vill hålla hemliga bör sparas på något annat ställe än i mobilens adressbok. Det finns tjänster, exempelvis hos Google, Apple och Microsoft, som gör det lätt att synkronisera adressboken mellan dator och mobiltelefon. En smidig lösning, men den innebär också att kontaktuppgifterna hamnar på servrar man som användare inte har någon kontroll över.

Dessutom finns det många andra tjänster² som vill komma åt innehållet i telefonens adressbok, bland annat för att hitta andra vänner som redan skaffat konto på samma tjänst.

Rensa i historiken

Har du använt mobiltelefonen för att leta upp kontaktuppgifterna till en person som du inte vill att andra ska veta att du har kontakt med eller för att skicka mejl, rensa bort de mest uppenbara spåren efteråt. Kommer någon över din telefon och tittar i webbläsarens historik eller vilka mejl som skickats har du i alla fall minskat risken att hen kommer över känsliga uppgifter.

Se upp med trådlösa nätverk

Koppla bara upp telefonen mot trådlösa nätverk som kräver kryptering, allra helst med standarden WPA2. Den teknik som heter WEP är lätt att hacka. Stäng också av funktionen som kopplar upp mobilen mot ett trådlöst nätverk automatiskt. Okrypterade nätverk är väldigt lätta att avlyssna för den som befinner sig i närheten. Från en dator är det bland annat möjligt att se vilka webbplatser du besöker och läsa den e-post du skickar och tar emot.

Telefonen letar efter kända nätverk

Ett annat problem med att låta telefonen koppla upp till trådlösa nätverk automatiskt är att det går att lura den att ansluta till en "falsk" basstation. Med wifi aktiverat skickar telefonen hela tiden ut namnet på alla trådlösa nätverk som finns sparade i inställningarna. Detta för att ett känt nätverk ska kunna upptäckas så snabbt som möjligt, men också för att telefonen ska kunna upptäcka basstationer, vars namn är dolda. Att telefonen söker efter kända nät på detta sätt är problematiskt ur flera aspekter. Det finns basstationer som kan lyssna efter "frågorna" som en telefon eller dator skickar ut och låtsas vara en av de basstationer som prylen söker efter. Resultatet är att den ansluter till basstationen och att trafiken därefter går att avlyssna av den som har kontrollen över den falska basstationen. I dagsläget är det bara nätanslutningar som är okrypterade eller skyddade med WEP som går att attackera på detta sätt. Men det räcker med att ett sådant nät finns med bland dem som telefonen söker efter för att den ska kunna luras.

Och även om det inte går att använda namnet på ett trådlöst nät skyddat med WPA2 för att få telefonen att koppla upp sig mot en falsk basstation går det att snappa upp att telefonen frågar efter de näten. Också det är ett potentiellt problem. Om två telefoner skickar ut samma ovanliga namn så är det åtminstone en indikation på att telefonerna, och då kanske även ägarna, har befunnit sig på samma plats. Det skulle kunna knyta två personer till varandra. Varje pryl med trådlöst nätverk har dessutom en unik adress som kallas

MAC-adress. Denna avslöjas när prylarna letar efter nätverk att koppla upp sig till. Genom att logga vilka MAC-adresser som funnits i närheten går det alltså att se när en viss telefon återkommer. Och har man lyckats ta reda på vilken MAC-adress en viss persons telefon har vet man alltså när hen med stor sannolikhet har befunnit sig på platsen.

Ett tredje problem är att det finns databaser som listar var i världen ett visst wifi-nätverk finns. Det är information som bland annat används för att förbättra mobiltelefonens positioneringsfunktioner. I stället för att bara förlita sig på gps går det att titta på vilka trådlösa nätverk som finns i närheten, det förbättrar precisionen och ger dessutom oftast snabbare resultat.

Men de här databaserna går också att använda omvänt: Genom att titta på vilka trådlösa nätverk en mobiltelefon frågar efter kan man med lite tur – om nätverken har unika namn och finns med i någon av databaserna – få veta var i världen just den basstationen finns.

Lösningen på alla problem som är kopplade till de här nätsökningarna är helt enkelt att stänga av wifi när du inte behöver den trådlösa uppkopplingen.

Stäng av Bluetooth

Det finns trojaner och annan skadlig kod som har smittat telefoner via Bluetooth. Om du inte använder tekniken, exempelvis för ett trådlöst headset, stäng av Bluetooth för att vara på den säkra sidan.

Kryptera telefonsamtalen

Normala mobilsamtal är inte skyddade mot avlyssning. Krypterad ip-telefoni är ett sätt att försvåra för den som vill försöka avlyssna ett telefonsamtal. Om internetuppkopplingen dessutom sker via en VPN-tunnel (se nästa avsnitt) komplicerar man det ytterligare för den som vill avlyssna en telefon.

I februari 2013 skrev Svenska Dagbladet en artikel³ som varnade för riskerna med telefonavlyssning i mobilnäten. Det som krävs är en bärbar basstation som lägger sig som en länk mellan mobiltelefonen och operatörens basstation. Tekniken gör det möjligt att avlyssna både röstsamtal och sms.

Lösningen är att kryptera både samtal och meddelanden. När detta skrivs är ett av de mest rekommenderade alternativen för detta Signal, en app som finns till både iPhone och Android. Den utvecklas av en programmeringsgrupp som heter Open Whisper Systems, där den i säkerhetskretsar kände Moxie Marlinspike är en av centralfigurerna.

Kryptera datakommunikationen

En smartphone är i många avseenden en dator, och därmed återfinns många av de säkerhetsproblem som är kopplade till en dator också i din ficka. Om kommunikation som går över internet, till exempel e-post eller chatt, inte är krypterad finns en risk att någon lyckas avlyssna den.

Avlyssningen kan ske på flera ställen. Är du uppkopplad mot ett trådlöst nätverk finns det en möjlighet för andra som befinner sig i närheten att tjuvlyssna på din Internettrafik. IT-avdelningen på källans arbetsplats har också stora möjligheter att läsa er kommunikation, precis som alla personer som har tillgång till nätverksutrustningen på vägen.

Kryptera nättrafiken

När du använder tjänster på internet, som e-post och känsliga webbplatser, se till att trafiken mellan din dator och servern är krypterad. I webbläsaren ska du använda adresser som börjar med https i stället för http, där "s" står för secure. Använder du inte en webbtjänst för din e-post utan i stället skriver och läser i telefonens e-postprogram ska du se till att det är inställt att skicka och ta emot e-post via en krypterad förbindelse.

Ett sätt att skaffa sig ytterligare ett skydd mot avlyssning är att använda ett så kallat VPN, ett virtuellt privat nätverk. Det är en teknik som innebär att all datatrafik som lämnar datorn krypteras. Det gäller även trafik som redan har krypterats av ett program i datorn, exempelvis HTTPS i webbläsaren.

För att kunna skydda dataförbindelsen med ett VPN krävs ett konto på en så kallad VPN-server. Viktigt är dock att det är en VPN-tjänst som använder en säker teknik. Det finns en äldre VPN-lösning som heter PPTP där det har hittats flera säkerhetshål. Den ska alltså undvikas helt. Man bör också välja bort VPN-tjänster som utvecklat egna lösningar och som kräver att tjänstens egna program är installerade på dator och mobiltelefon. Det finns öppna, väl beprövade lösningar som är att föredra. Open VPN och IPSec är två alternativ.

I valet av VPN-tjänst är det viktigt att fundera på vem det är man vill skydda sig mot. Med ett VPN läggs ett extra krypteringslager på i kommunikationen mellan telefon (eller dator) och VPN-server. Servern plockar sedan bort krypteringen och skickar datainnehållet vidare till destinationen. Om inte även det som skickas i VPN-tunneln är krypterat, exempelvis med HTTPS för webbtrafik, finns därmed en risk att den som sköter VPN-servern avlyssnar trafiken. Om det av någon anledning finns skäl att misstänka att den du vill skydda

dig mot har inflytande över en VPN-tjänst som du överväger att använda bör du därför välja en annan.

En fördel med en VPN-tunnel är att den förflyttar det potentiella läckaget till en annan geografisk plats än den där användaren befinner sig. På det lokala kaféet kan någon känna igen dig och få för sig att försöka avlyssna trafiken. Men med en VPN-tjänst som befinner sig långt bort, kanske till och med i ett annat land, blir det svårare att koppla kommunikation till en viss person. Ett annat sätt att minska riskerna med avlyssning av någon som befinner sig i närheten är att slå av telefonens trådlösa nätverk och i stället bara låta den kommunicera via 3G.

När man använder VPN i mobiltelefonen gäller det att vara vaksam på att många appar börjar skicka data redan innan VPN-förbindelsen är upprättad. Först när telefonen fått kontakt med VPN-servern skickas data den krypterade vägen.

Ett sätt att kontrollera om VPN-förbindelsen fungerar är att använda en tjänst som <http://whatismyipaddress.com> och jämföra resultatet med och utan VPN-anslutning. Tjänsten visar vilken ip-adress din dator eller mobiltelefon identifierar sig med på nätet. Med och utan VPN-tunnel ska det vara två olika ip-adresser.

Ett alternativ till kommersiella VPN-serverar är Tor⁴, en gratistjänst som utvecklas med bidrag från bland annat Sida, som gör det möjligt att surfa anonymt.

Precis som med VPN-lösningar krävs dock att trafiken som skickas via Tor är krypterad. Annars finns det en risk att trafiken avlyssnas när den väl lämnat Tor och fortsätter till destinationen.

Tor finns till Android-telefoner. Med Orbot installerat går det att dölja sin ip-adress och till viss del skydda datatrafiken med kryptering. Men det krävs en så kallad root:ad mobiltelefon för att all trafik ska gå via Tor. I normala fall går bara viss trafik via Tor. Surfar man exempelvis med Chrome kommer webbtrafiken, trots att Orbot är installerat i telefonen, att vara oskyddad, medan den som i stället använder webbläsaren Orweb kommer att vara anonymiserad.

I bästa fall ska förbindelsen alltså vara krypterad i flera steg: WPA2 krypterar den trådlösa kommunikationen mellan mobiltelefon och basstation, VPN eller Tor krypterar trafiken från telefonen och en bit ut på nätet medan HTTPS eller liknande krypterar trafiken från programmen i telefonen och fram till destinationen.

Genom att på detta sätt lägga på kryptering i flera lager skaffar man sig som användare ett förstärkt skydd mot dem som kan tänkas försöka avlyssna trafiken. Råkar man exempelvis använda en okrypterad webbplats för att skicka känslig information så ger WPA2 och VPN-tunneln fortfarande ett skydd, åtminstone en bit av vägen.

Kryptera e-posten

E-posten ska helst krypteras på två sätt. Den kryptering som det oftast pratas om är lösningar som Pretty Good Privacy, PGP⁵. Med PGP krypteras själva innehållet i ett mejl. Därmed blir det omöjligt för en utomstående som lyckas snappa upp ett mejl att se vad två parter skriver till varandra. Men det är fortfarande möjligt att se vilka det är som kommunicerar och mejlets ärenderad. Adresserna, både mottagarens eller avsändarens, är fortfarande i klartext. Skulle också adresserna vara krypterade skulle nämligen mejlet inte hitta fram.

Att innehållet i känslig e-post bör vara krypterad beror på att ett mejl på vägen från avsändare till mottagare passerar väldigt många steg. Och i varje hopp har it-teknikerna i teorin möjlighet att läsa innehållet i brevet.

Tyvärr är det fortfarande ganska bökigt att skicka och ta emot krypterad e-post i mobiltelefonen. För säker kommunikation på språng är redan nämnda Signal ett bättre alternativ.

För att skydda sin e-post ytterligare bör man också se till att kommunikationen mellan den egna mobiltelefonen och e-postservern är krypterad. Använder man en webbtjänst för sin e-post, som Googles Gmail, bör man surfa till en krypterad sida innan man matar in sitt lösenord. Adressen ska börja med https:// i stället för http://. Använder man ett e-postprogram i telefonen ska man i stället se till att förbindelsen till e-postservern skyddas med teknik som TLS eller SSL.

Om kommunikationen mellan telefon och e-postserver/webbtjänst inte är krypterad innebär det att användarnamn och lösenord skickas i klartext. Det innebär i sin tur att andra personer ibland kan snappa upp inloggningsuppgifterna. Och då hjälper det inte längre hur långt och komplicerat lösenord man än har valt.

Välj webb före app

Om du använder telefonens webbläsare kan du själv kontrollera att förbindelsen till nättjänsten använder en krypterad HTTPS-förbindelse. Om en installerad app skickar data krypterat eller okrypterat är svårare att veta. Ska du hantera känslig information, välj därför hellre en HTTPS-anslutning i webbläsaren i stället för en app om det är möjligt.

Fabriksåterställning raderar inte alla data

Många telefoner har en funktion för så kallad fabriksåterställning. Syftet är att alla data från telefonen ska raderas, så att den till exempel ska gå att sälja i andra hand utan att säljarens information hamnar i köparens händer.

Men en granskning⁶ som tidningen Computer Sweden gjorde vintern 2013 visar att funktionen inte alltid fungerar som användarna förväntar sig. Tidningen gav ett säkerhetsföretag i uppdrag att försöka återskapa information från begagnade telefoner som köpts på Blocket, och resultatet var nedslående.

Säkerhetsexperterna lyckades bland annat att återskapa mötesanteckningar, kontaktlistor och fotografier.

Malware stjäl information

Till datorer har det under lång tid funnits olika typer av spionprogram som bland annat kan användas för att stjäla inloggningsuppgifter och annan information.

Motsvarande program börjar nu dyka upp också till mobiltelefoner. Främst är det Android som är drabbat. Det du som användare kan göra för att minska risken för att råka installera ett spionprogram är att bara ladda ner nya appar från pålitliga källor, som Googles egen appbutik Google Play. Du bör också titta igenom vilka rättigheter appen begär när du installerar den, och avbryta installationen om ett program utan uppenbar anledning exempelvis vill komma åt telefonens adressbok.

Försiktigt med molntjänsterna

Nätets molntjänster kan förenkla datoranvändningen ordentligt. I begreppet "molntjänster" ryms en mängd olika lösningar. Det de har gemensamt är att data lagras på nätet i stället för i användarens dator. Exempel på molntjänster är Dropbox som fungerar som en hårddisk och Google Drive, sökjättens lösning för ordbehandling och kalkylblad som tidigare hette Google Docs.

Men ur ett integritetssperspektiv kan molntjänsterna vara problematiska. Som användare tvingas man lita på att företaget som tillhandahåller tjänsten har koll på säkerheten. Och historien visar att så inte alltid är fallet. Dessutom ligger informationen ofta lagrad på servrar i andra länder än Sverige, där annan lagstiftning gäller.

Allmän försiktighet med alla typer av molntjänster rekommenderas därför för känslig information. Men det kan också finnas tillfällen då molntjänster är ett betydligt bättre alternativ än att lagra dokument och bilder på den egna datorns hårddisk. Ett exempel är om

du ska resa in i eller ut ur länder där det finns en risk att innehållet på hårddisken kontrolleras. Att då jobba mot en molntjänst, gärna via en Tor-uppkoppling, är ett bra alternativ. Som alltid: Eftersom hotbilden varierar från jobb till jobb är vissa lösningar bra ibland, men ibland dåliga.

Mobilnätet vet var telefonen är

Mobiltelefonen kan på olika sätt och med varierande grad av noggrannhet avslöja var i världen du befinner dig. Av tekniska skäl behöver mobilnätet veta var varje mobiltelefon befinner sig. Det är den möjligheten polisen använder när de söker efter folk.

Det finns också teknisk utrustning, så kallade *IMS/ catchers*, som kan användas för att lokalisera en specifik telefon om den befinner sig i närheten. Det är fortfarande relativt dyr utrustning, men priserna på teknik går ju alltid ner.

IP-adresser ger ungefärlig plats

Varje pryl som är uppkopplad till internet har en ip-adress. Dessa IP-adresser går ofta att koppla till en ungefärlig geografisk plats, ibland till ett visst företag. Besöker du en webbplats när du är uppkopplad via ett nätverk är sannolikheten stor för att företaget eller personerna som driver webbplatsen i sina loggfiler kan se att de fått besökare från nätverket.

Tor kan användas för att försvåra avlyssning av datatrafiken, men verktyget ger också uppkopplade prylar en annan ip-adress än de "egentligen" har. Tor kan därmed ge utökad anonymitet på nätet.

Insamling av MAC-adresser

Varje pryl som kan kopplas till ett nätverk – trådbundet eller trådlöst – har en så kallad MAC-adress som är unik. Varje gång mobiltelefonen söker efter ett trådlöst nätverk att koppla upp sig emot meddelar den också vilken MAC-adress den har.

Det finns företag som utvecklar kommersiella lösningar som utnyttjar detta. Tanken är att butiksägare ska kunna se hur kunder rör sig i butiken, hur ofta de återvänder och på andra sätt få användbar statistik. Men man kan också tänka sig en situation där möjligheten används för att se om en viss person befunnit sig på en viss plats.

Lösningen är att stänga av wifi när den trådlösa uppkopplingen inte behövs.

Positionering med gps

Allt fler appar i telefonen använder gps:en för att lägga till uppgifter om latitud och longitud i exempelvis bilder eller statusuppdateringar i sociala nätverk.

Innan du publicerar bilder på webben eller skickar dem till någon annan, kontrollera därför att det inte finns med känsliga uppgifter i metainformationen. Det kan bland annat göras i datorn. I en Mac, öppna bilden i programmet *Förhandsvisning*, välj *Visa granskare* i *Verktygsmenyn* och klicka sedan på fliken för mer information (visas som ett gement i inuti en svart ring). Om bilden har gps-information syns det där. I Windows, högerklicka på bilden i *Utforskaren*, välj *Egenskaper* och sedan *Detaljer*. Bläddra nedåt i informationen, där syns gps-data om det finns.

För att kunna ta bort eventuell gps-information i bilden behövs en så kallad EXIF-redigerare. Sådana program finns till både Mac och Windows, men också till Android och Iphone.

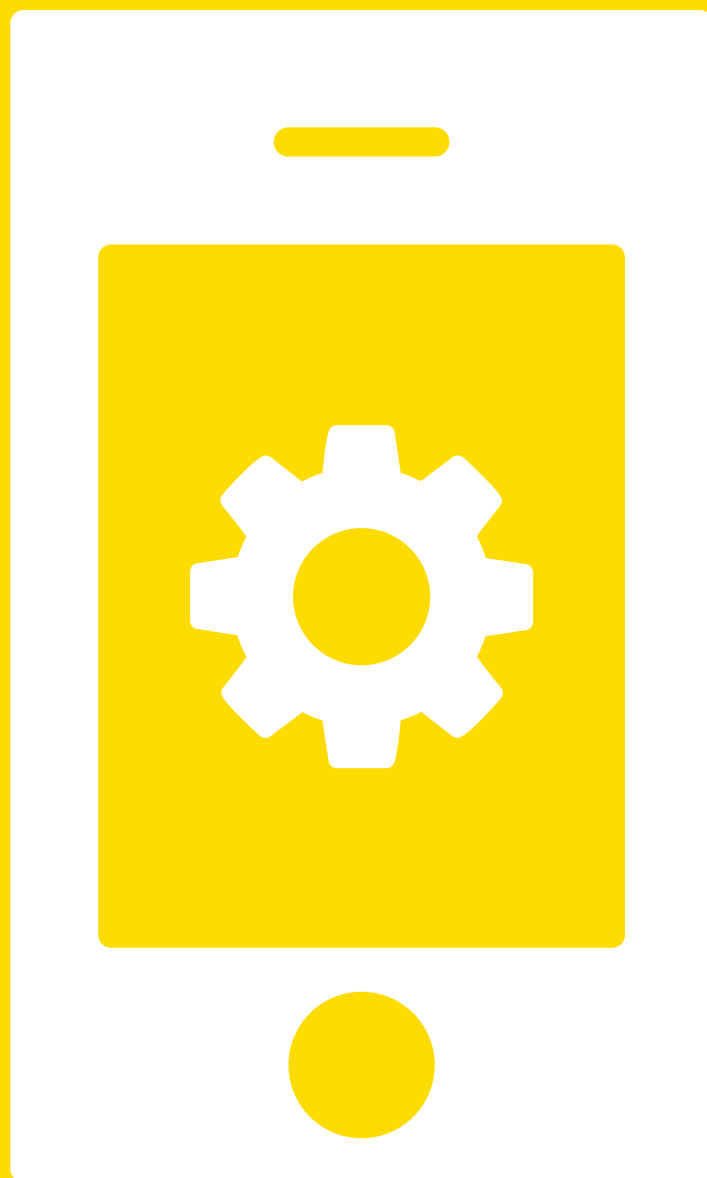
Gå även igenom inställningarna för de appar som finns installerade i telefonen och kontrollera vilka som över huvud taget får använda gps:en.

Skydda röstbrevlådan med en pinkod

Ringer du till din röstbrevlåda från en annan telefon behövs en fyrsiffrig pinkod för att kunna lyssna av nya meddelanden. Om du däremot inte har aktiverat funktionen krävs ingen pinkod om du ringer från ditt eget nummer. I stället ser operatören att du ringer från rätt nummer och släpper in dig direkt.

Men det finns teknik som gör det möjligt att visa ett annat telefonnummer än det man faktiskt ringer i från. Genom att använda ditt mobilnummer kan det därmed vara möjligt för någon annan att avlyssna din röstbrevlåda om den inte är skyddad av en pinkod, oavsett från vilket nummer denna någon ringer. Det innebär också att säkerheten för röstbrevlådan inte kan bli starkare än en fyrsiffrig kod.

Inställningar för din telefon



iPhone

1

Samtliga inställningar för Iphone görs i appen *Inställningar*.

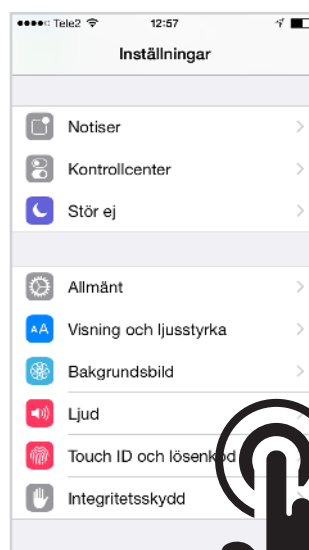


2

Lösenkodlås

Med ett lösenord krävs en fyrsiffrig kod för att kunna låsa upp telefonen.

I *Inställningar*, klicka på *Touch ID och lösenkod*.



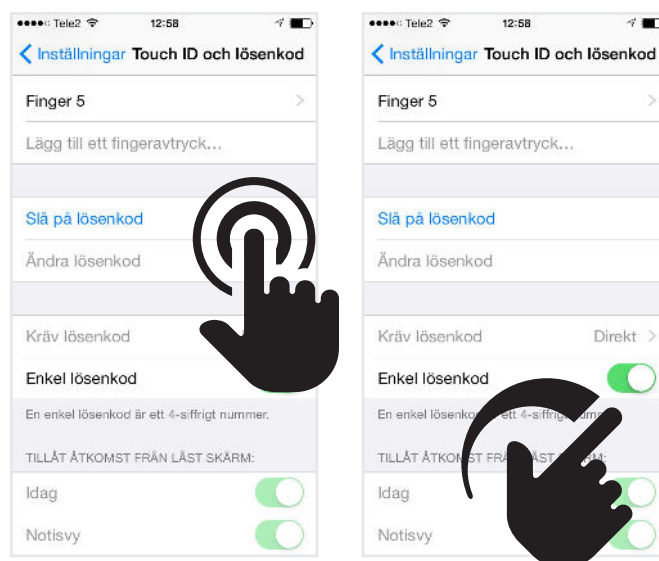
2.1

Klicka på *Slå på lösenord* och mata in den fyrsiffriga kod du vill använda två gånger. När du har valt kod kan du också ställa in hur lång tid det ska gå att låsa upp telefonen utan att mata in lösenordet. Valet här är en avvägning mellan bekvämlighet och säkerhet. Ju kortare tid, desto mindre lucka lämnar du för någon som kommer över din telefon, men desto oftare måste du själv mata in koden för att använda telefonen. Möjligen ökar dock risken för att någon tittar över din axel och ser vilken kod du har.

I den här vyn kan du också välja att aktivera fingeravtrycksläsaren, om du har en Iphone 5S eller senare. Du kan också välja vilka funktioner i telefonen som ska gå att använda när den är låst. Längst ned finns alternativet *Radera data*.

Aktivera detta. Då kommer alla data som finns i telefonen att raderas om någon gör tio misslyckade försök att låsa upp den.

Genom att stänga av *Enkel lösenkod* kan ett ord eller teckenkombination av valfri längd väljas i stället för en fyrsiffrig kod.



3

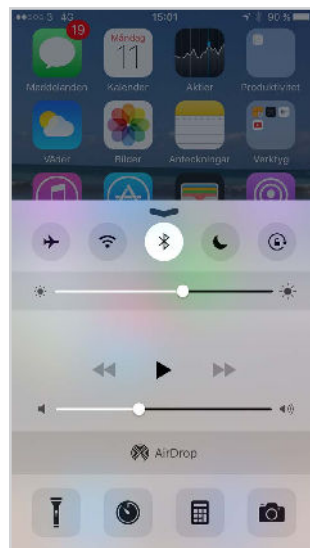
Stäng av Bluetooth

I *Inställningar*, välj *Bluetooth* och slå av funktionen.



3.1

Det går också att svepa in över skärmen från utsidan av dess nederkant. Då visas en panel med diverse genvägar, bland annat en för att sätta på och stänga av Bluetooth.

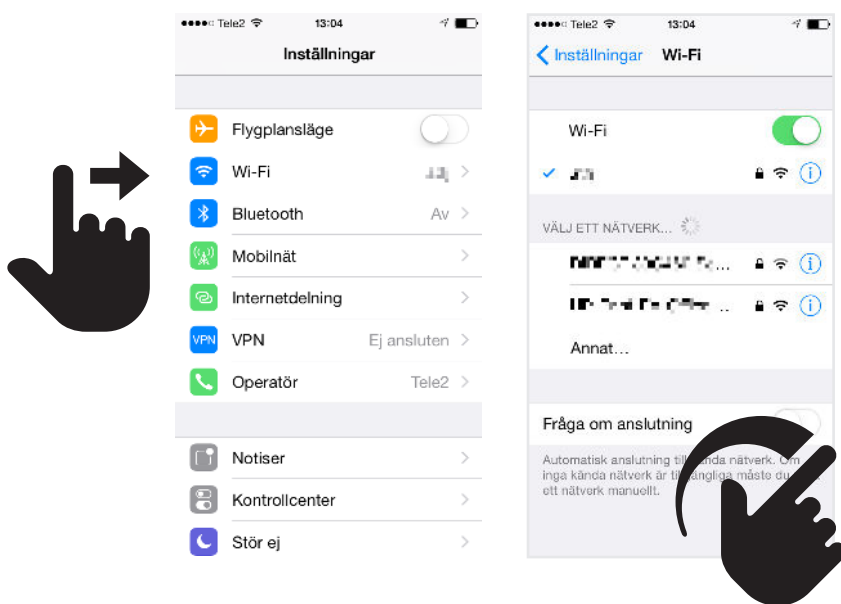


4

Stäng av det trådlösa nätverket

I *Inställningar*, klicka på *Wi-Fi*. Använd det översta reglaget för att stänga av det trådlösa nätverket i telefonen. Även det trådlösa nätverket går att slå av och på i panelen med genvägar.

Koppla inte upp automatiskt. Telefonen har en funktion som gör att den automatiskt kopplar upp till nätverk som den tidigare har varit ansluten till. Det går att stänga av den funktionen, så att man i stället får en fråga om man verkligen vill ansluta. Aktivera *Fråga om anslutning* på den högra bilden.



5

Välj krypterade nät

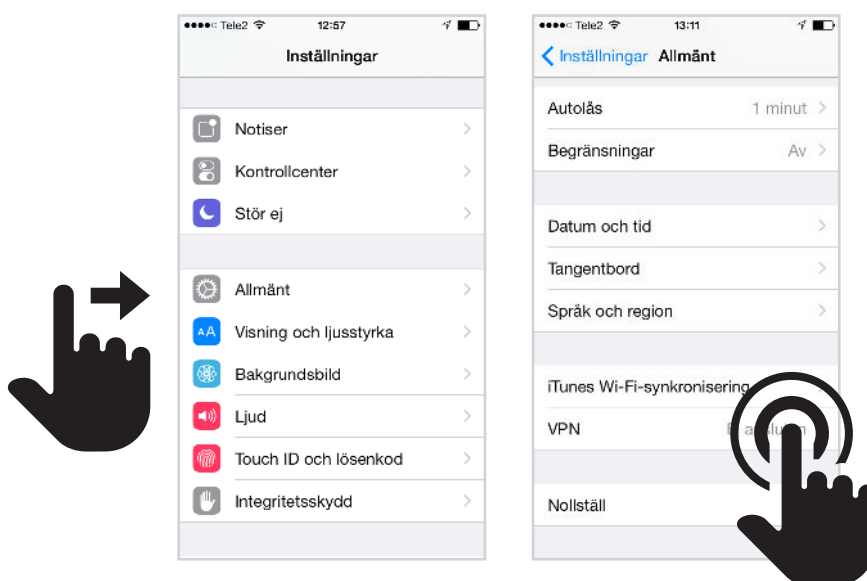
I listan med trådlösa nätverk som finns i närheten visar ett säkerhetslås att det är ett nät som är krypterat. Välj alltid att koppla upp till krypterade nätverk. I ett nätverk som inte är krypterat ökar risken för att någon avlyssnar datatrafiken.



6

Använd VPN

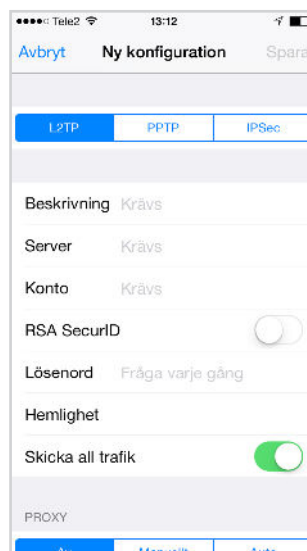
I *Inställningar*, välj *Allmänt*. Klicka på VPN.



6.1

Klicka på *Lägg till VPN-konfiguration*. Välj sedan *L2TP*, *PPTP* eller *IPSec* beroende på vilken typ av VPN-förbindelse som ska användas. Undvik *PPTP*, då det är en teknik med flera kända säkerhetsbrister. Om VPN-tjänster du använder bygger på en teknik som heter *OpenVPN* måste du ladda ner OpenVPN-appen från App Store.

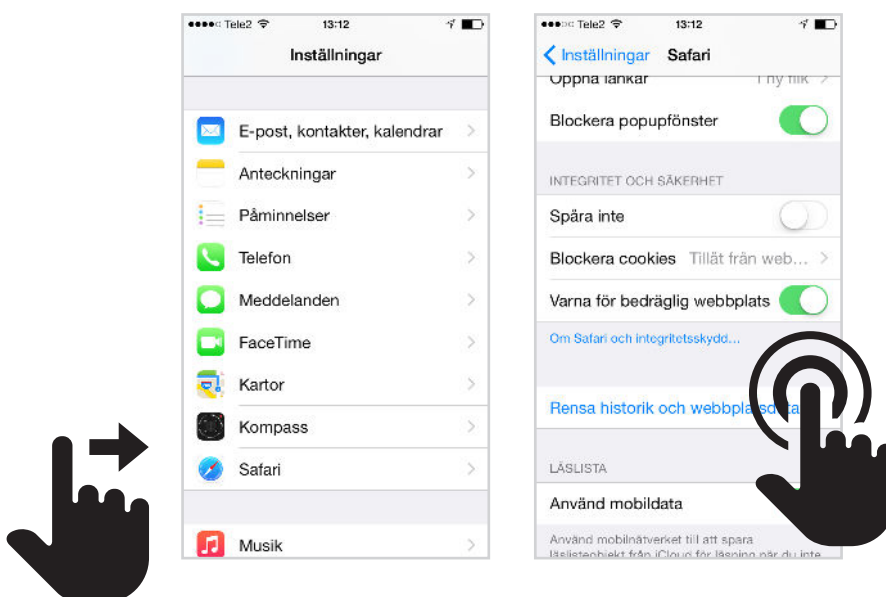
Mata sedan in de uppgifter som du fått från it-avdelningen eller VPN-tjänsten.



7

Rensa surfhistoriken

I *Inställningar*, välj *Safari*. Välj *Rensa historik och webbplatsdata*. Använder du någon annan webbläsare än Safari finns motsvarande funktion för att rensa i surfhistoriken.



8

Krypterad surf

När du använder webbläsaren, använd om möjligt adresser som börjar med HTTPS i stället för HTTP. Överföringar via HTTPS är skyddade med kryptering och försvårar därför för den som vill försöka avlyssna din webbtrafik.

Att förbindelsen till webbservern är krypterad indikeras av en ikon i form av ett hänglås i adressfältet.

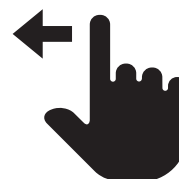
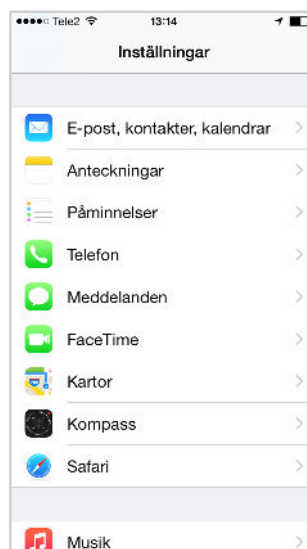


9

Krypterad koppling till e-postservern

Om du använder telefonens e-postprogram är det en bra idé att se till att mejlen hämtas och skickas via en krypterad förbindelse.

I *Inställningar*, välj *E-post*, *kontakter*, *kalendrar*.



Krypterad koppling till e-postservern

Välj det konto du vill ändra inkommande inställningar för. Klicka dig vidare till inställningarna. Välj *Avancerat*. Aktivera *Använd SSL*. För att kryptera förbindelsen när e-post skickas, välj *SMTP* och sedan den server som används. Aktivera *Använd SSL*.

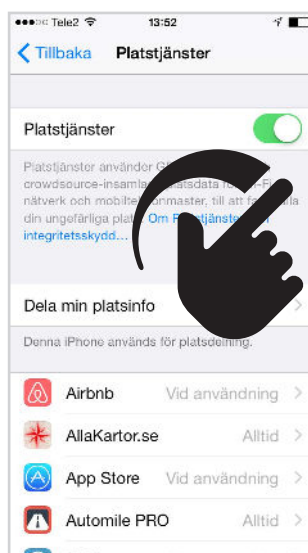
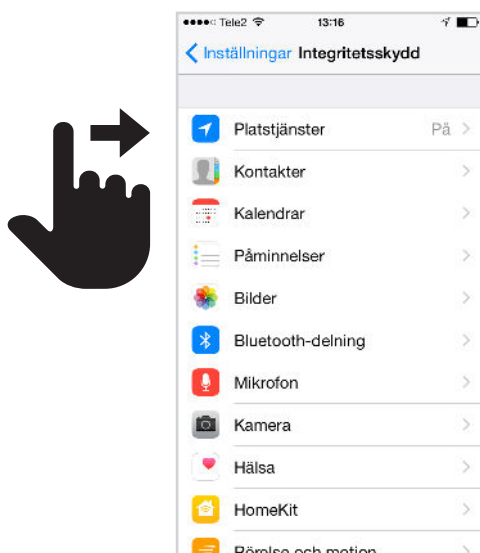
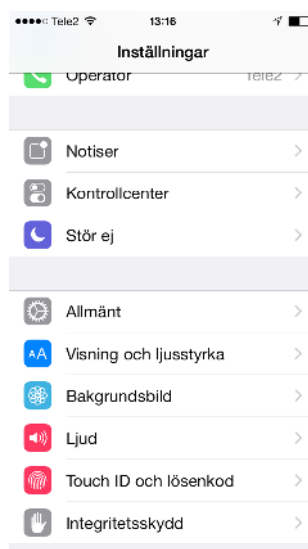


10

Positionering – slå av gps-funktionen

För att hindra alla appar i telefonen från att använda positioneringstjänster, välj *Integritetsskydd* i *Inställningar*.

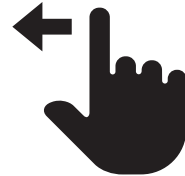
Välj *Platstjänster*. Inaktivera *Platstjänster* överst på sidan.



10.1

Positionering - appinställningar

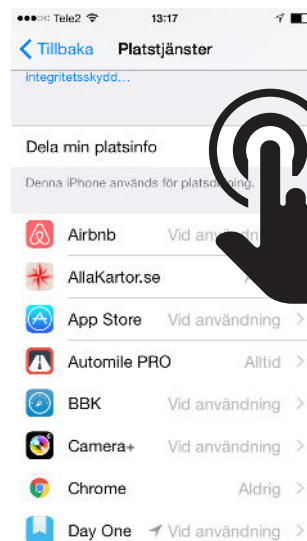
Om du vill använda gps:en ihop med somliga appar men inte andra, lämna *Platstjänster* aktiverat och slå i stället av funktionen för de aktuella apparna i listan.



10.2

Positionering - visa var din telefon är

Dela min platsinfo är en funktion som gör det möjligt för utvalda personer att se var din telefon befinner sig. Under det här alternativet sköter du inställningarna för den möjligheten.

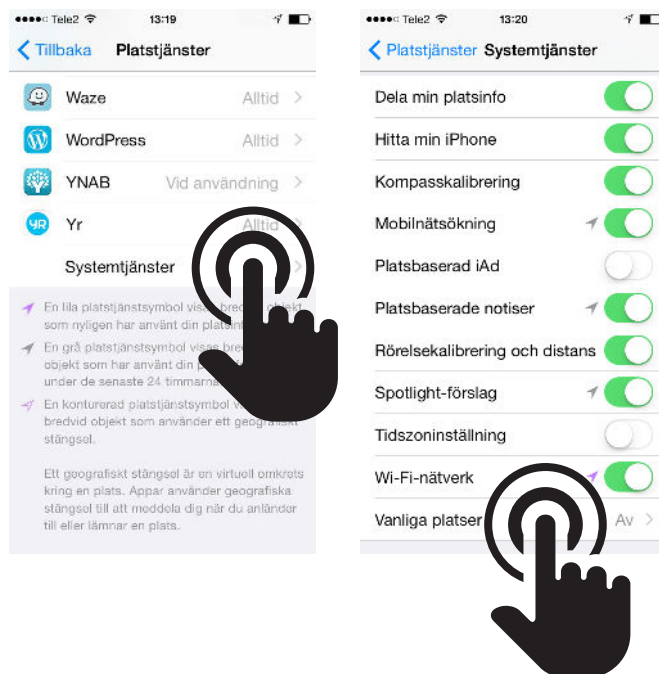


10.3

Positionering – vanliga platser

Funktionen vanliga platser registrerar var du ofta befinner dig. Enligt Apple lämnar uppgifterna aldrig telefonen, men för dig eller för en källa kan det vara problematiskt nog att de finns där.

Längst ned i inställningarna för platstjänster finns alternativet *Systemtjänster*. Här finns möjlighet att välja hur funktioner som finns inbyggda i telefonen får använda platstjänster. Längst ned i listan finns möjligheten att stänga av *Vanliga platser*.

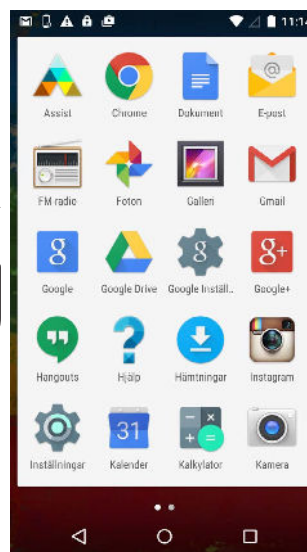


Android

1

Eftersom Android är ett öppet operativsystem som telefon-tillverkarna har möjlighet att anpassa är det inte säkert att inställningarna i just din telefon har samma namn och finns på samma ställe som i instruktionerna nedan. Instruktionerna är baserade på Android 5.1. Motsvarande inställningar ska dock finnas, oavsett telefon-modell.

Alla inställningar görs i appen *Inställningar*.

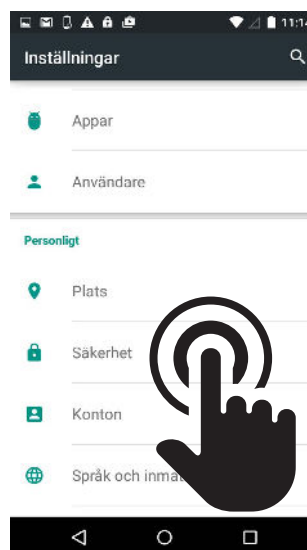


2

Skärmlås

Med skärmlås kan den som hittar telefonen inte bara börja använda den. På Android telefoner finns flera varianter av skärmlås:

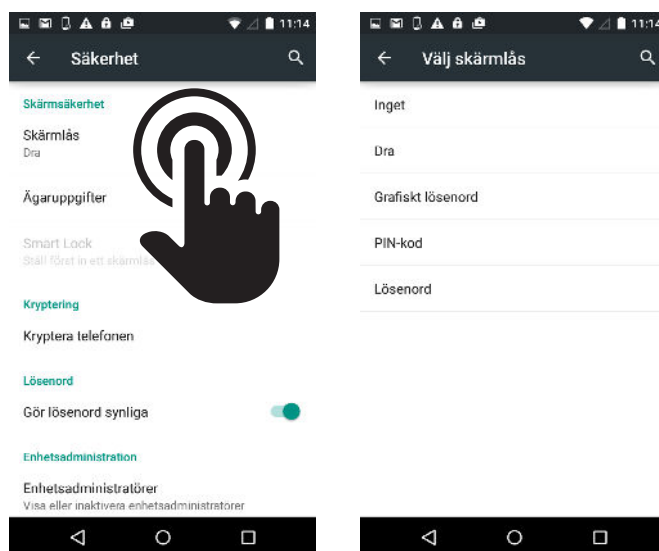
- Pinkod – fyrsiffrig kombination.
- Lösenord – valfritt lösenord, minst fyra tecken långt.
- Grafiskt lösenord – innebär att man ska dra streck mellan minst fyra av nio punkter på skärmen.



Det finns också en möjlighet att använda ansiktsgenkänning som kod, men det har förekommit diskussioner på nätet om hur enkel den varianten är att lura med hjälp av ett fotografi. Den som väljer att ställa in ett så kallat *Ansiktslås* varnas också för att det inte är en lika säker lösning som de tre ovanstående.

I *Inställningar*, klicka på *Säkerhet*. Under *Skärmsäkerhet*, välj *Skärmlås*.

Ställ sedan in den variant du vill använda. I rutan som dyker upp väljer du vilka typer av aviseringar, det vill säga meddelanden från dina installerade appar, som ska visas på låsskärmen.

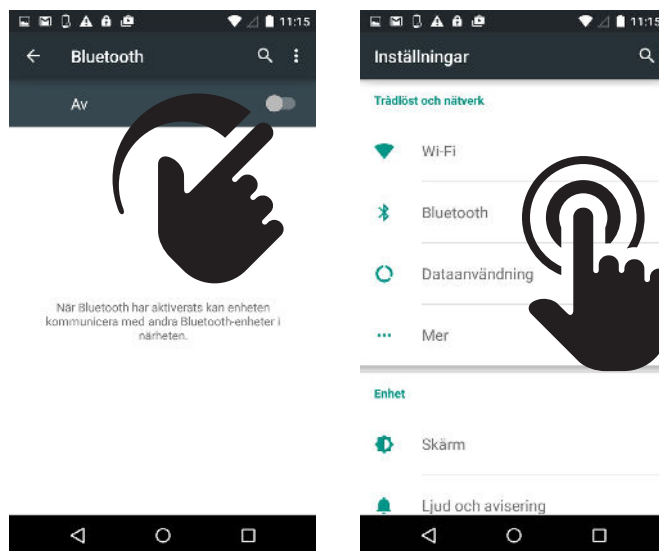


Har du en äldre version av Android, gå också in i alternativet *Utvecklare* i *Inställningar* och kontrollera att ADB inte är aktiverat. ADB är en funktion som utvecklare använder och som bland annat innebär att det går att komma åt informationen på en telefon med skärmlås om den kopplas till en dator. På nyare versioner av Android finns inte menyalternativet för ADB kvar. Funktionen aktiveras i stället på ett annat sätt, just för att den inte ska kunna bli påslagen av misstag.

3

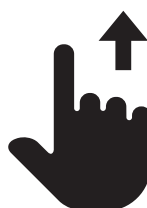
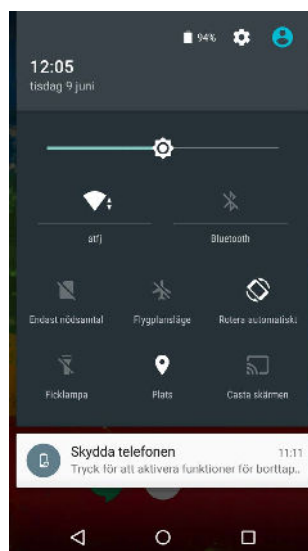
Stäng av Bluetooth

I *Inställningar*, välj *Bluetooth*. Välj sedan att slå på Bluetooth.



3.1

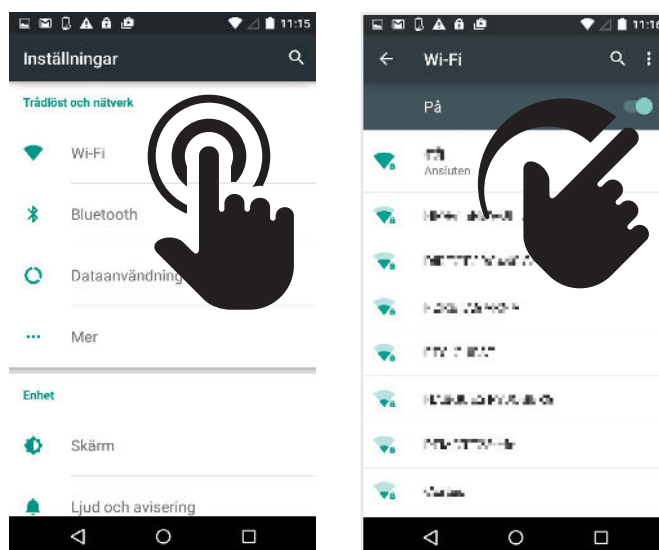
Bluetooth kan också stängas av och slås på från panelen med genvägar som du kommer till genom att svepa ned från skärmens överkant.



4

Stäng av det trådlösa nätverket

I *Inställningar*, välj *Wi-Fi*. Använd reglaget överst för att slå på och av wifi. Du kan också komma åt den inställningen från samma panel med genvägar som du använder för Bluetooth.

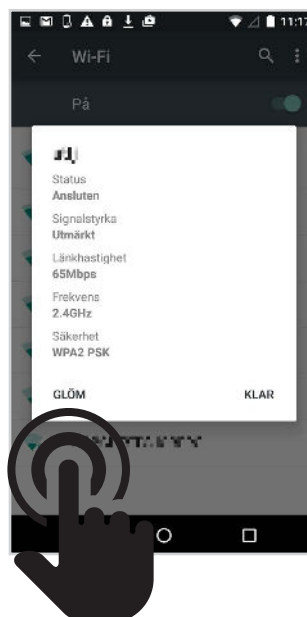


5

Koppla inte upp automatiskt

I Android finns ingen inbyggd funktion som förhindrar att telefonen automatiskt kopplar upp sig till kända trådlösa nätverk. Alternativen är antingen att stänga av wifi eller att radera de nätverk som man inte vill återansluta till.

När du gått in i inställningarna för wifi, klicka på det nätverk du vill radera och välj *Glöm* i rutan som dyker upp.

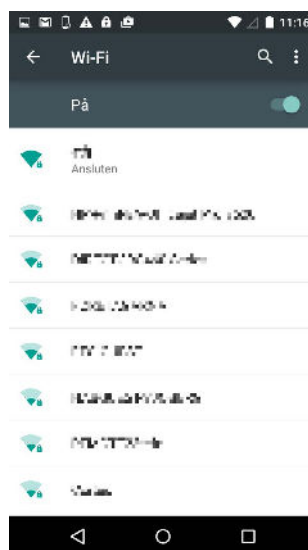
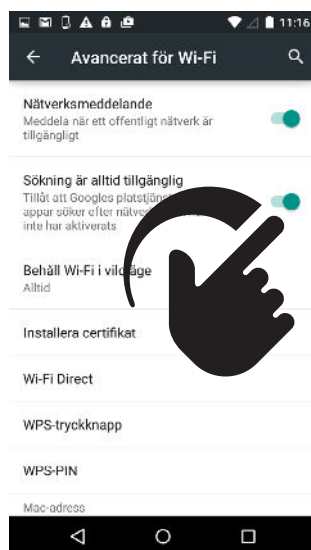
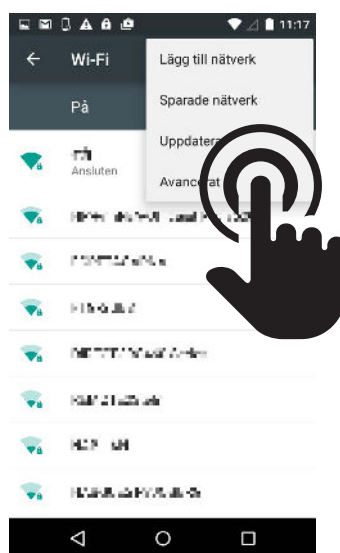


Precis som i en Iphone samlas information om var du och din telefon befinner er. Med denna funktion aktiverad kommer vissa funktioner i telefonen att använda wifi för att bland annat positionera telefonen. Det innebär också att telefonens MAC-adress kontinuerligt skickas ut.

Om du vill stänga av funktionen, klicka på de tre punkterna i övre högra hörnet ovanför listan med dina kända nätverk och välj *Avancerat*.

Stäng sedan av *Sökning* är *alltid tillgänglig*.

Välj *Krypterade nät*.



I listan med trådlösa nätverk som finns i närheten visar ett hänglås att det är ett nät som är krypterat. Välj alltid att koppla upp till krypterade nätverk. I ett nätverk som inte är krypterat ökar risken för att någon avlyssnar datatrafiken.

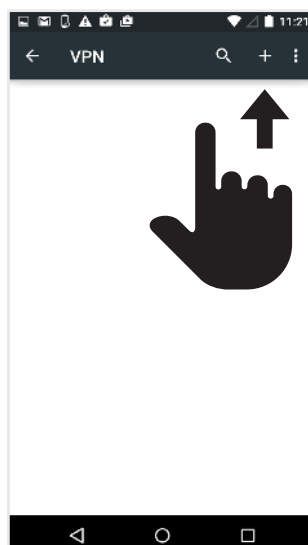
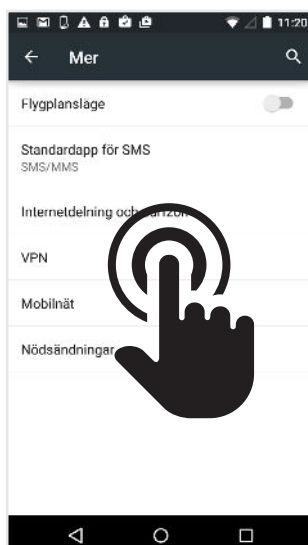
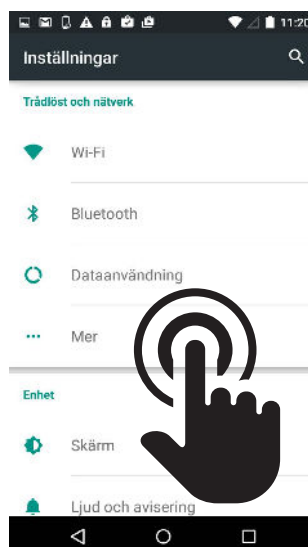
6

Använd VPN

I *Inställningar*, välj *Mer* direkt under *Dataanvändning*.

Klicka på *VPN*. En ny VPN-anslutning lägger du till genom att klicka på plus-tecknet. Välj sedan den typ av VPN-förbindelse som ska användas. Undvik PPTP, då det är en teknik med flera kända säkerhetsbrister.

Mata in de uppgifter som du fått av it-avdelningen eller VPN-tjänsten.



7

Rensa surfhistoriken

I webbläsaren Chrome, klicka på de tre prickarna i övre högra hörnet. Välj *Inställningar* och därefter *Sekretess*. Välj *Rensa webb-information* i övre delen av skärmen. Markera den information du vill radera och tryck på Rensa.

Använder du en annan webbläsare än Chrome finns motsvarande funktion för att rensa i surfhistoriken.



8

Krypterad surf

När du använder webbläsaren, använd om möjligt adresser som börjar med HTTPS i stället för HTTP. Överföringar via HTTPS är skyddade med kryptering och försvårar därför för den som vill försöka avlyssna din webbtrafik.

Att förbindelsen till webbservern är krypterad indikeras av en ikon i form av ett hänglås i webbläsarens adressfält.



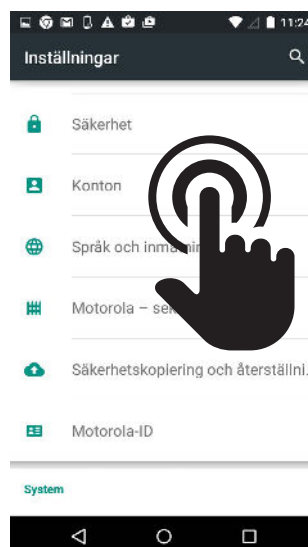
9

Krypterad koppling till e-postservern

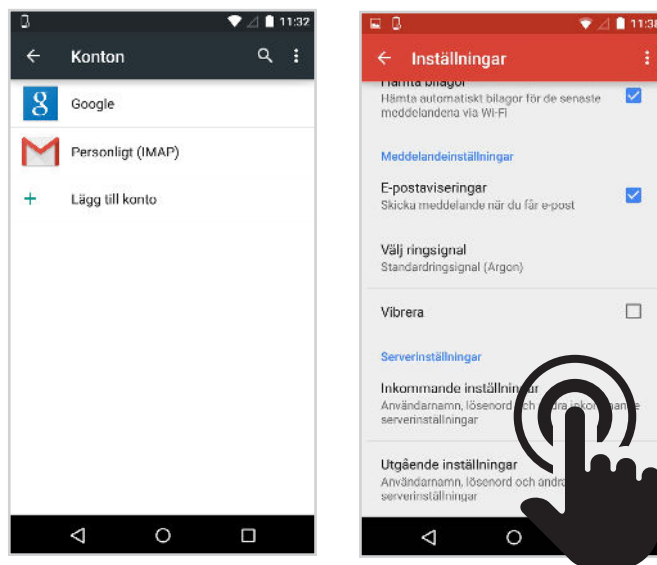
Om du använder telefonens e-postprogram är det en bra idé att se till att mejlen hämtas och skickas via en krypterad förbindelse.

I *Inställningar*, välj *Konton*.

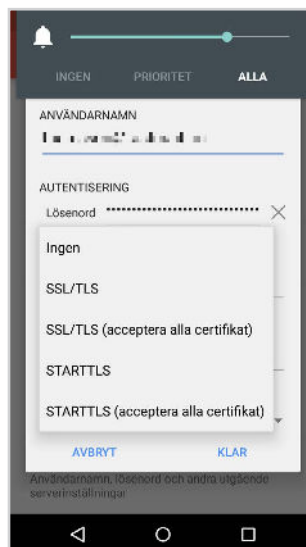
Klicka på rätt konto och sedan på *Kontoinställningar*. Välj sedan rätt konto igen. Välj *Inkommande inställningar*.



Inställningar för din telefon: Android



Klicka på *Säkerhetstyp* och välj den krypteringsmetod som e-posttjänsten använder. Gör sedan motsvarande val för *Utgående inställningar*.



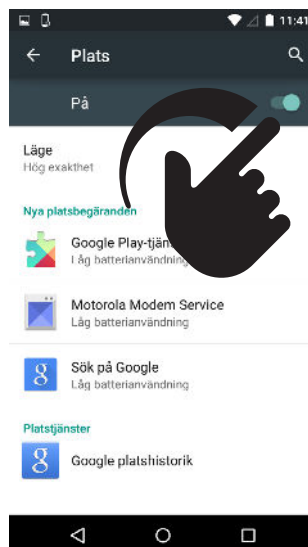
På Android finns också möjlighet att ta emot och skicka e-post krypterad med PGP, om du installerar PGP-appen AGP och e-post-appen K9.

10

Positionering – slå av gps-funktionen

För att hindra att alla appar i telefonen använder positioneringstjänster, välj *Plats* i *Inställningar*. Inaktivera därefter *Plats*.

På Android i standardutförande finns ingen möjlighet att begränsa tillgången till gps:en app för app.



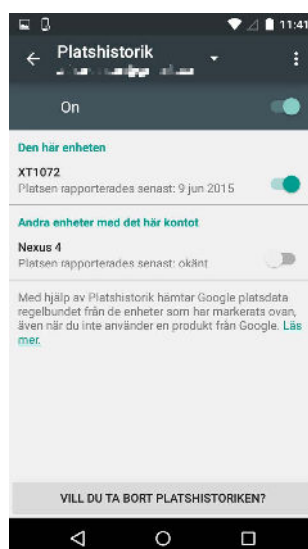
10.1

Positionering – platshistorik

Funktionen *Platshistorik* registrerar var din telefon och därmed sannolikt också du befinner dig. Google använder informationen bland annat för sin tjänst Google Now och för att förbättra både sökresultat och annonser.

Informationen skickas till Googles servrar och görs bland annat tillgänglig för dig på <https://maps.google.com/locationhistory>.

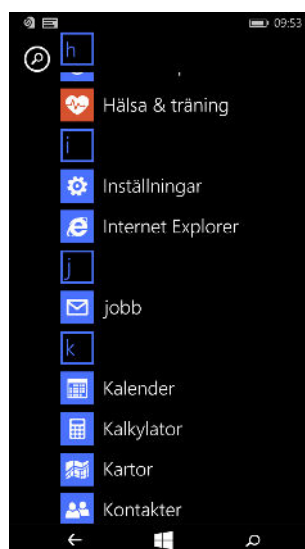
Välj *Platshistorik* längst ned i *Plats* och slå sedan av funktionen om du inte vill använda den.



Windows Phone

1

Samtliga inställningar för Windows Phone görs i appen *Inställningar*. Instruktionerna här gäller Windows Phone 8.1.



2

Lösenord

Med ett lösenord krävs en sifferkod för att kunna låsa upp telefonen.

I *Inställningar*, klicka på *Låsskärm* under rubriken *Anpassning*.

Skrolla ner och välj att slå på lösenordet. Mata sedan in den sifferkombination du vill använda. Observera att den kan vara mer än fyra siffror lång.





När du gjort det kan du ställa in hur lång tid det ska gå att låsa upp telefonen utan att mata in lösenordet under *Kräv lösenord*. Valet här är en avvägning mellan bekvämlighet och säkerhet. Ju kortare tid du anger, desto mindre lucka lämnar du för någon som kommer över din telefon, men ju oftare måste du själv mata in koden för att använda telefonen.

3

Stäng av Bluetooth

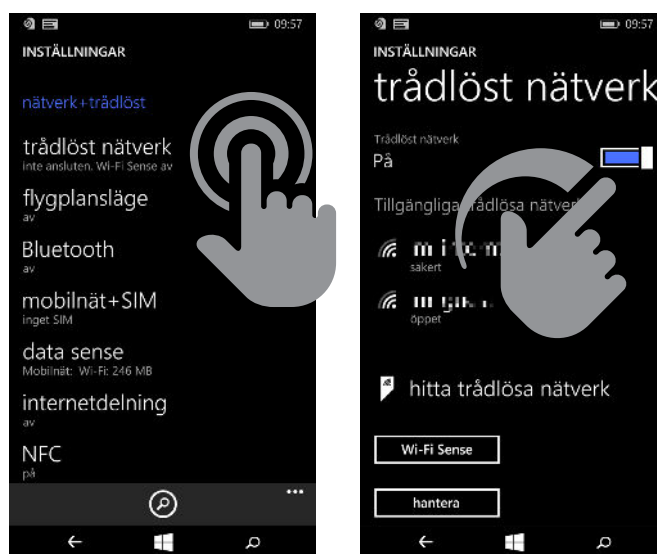
I *Inställningar*, under *Nätverk + trådlöst*, välj *Bluetooth* och slå av funktionen.



4

Stäng av det trådlösa nätverket

Under *nätverk + trådlöst* kan du klicka på *Trådlöst nätverk*. Använd det översta reglaget för att stänga av det trådlösa nätverket i telefonen.



5

Koppla inte upp automatiskt

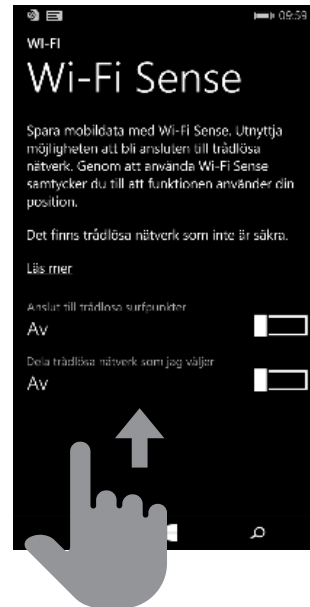
Telefonen har en funktion som gör att den automatiskt kopplar upp sig till nätverk som den tidigare har varit ansluten till. Det går att stänga av funktionen, så att du i stället får en fråga om du verkligen vill ansluta.

I *Inställningar*, klicka på *Trådlöst nätverk* och gå vidare till *Avancerat*. Stäng av funktionen *Anslut automatiskt till trådlösa surfpunkter*.

Längre ner på samma sida går det att radera de trådlösa nätverk du inte längre vill att telefonen ska leta efter. Klicka på *Hantera*, välj de nätverk du vill radera och klicka avslutningsvis på *soptunnan*.



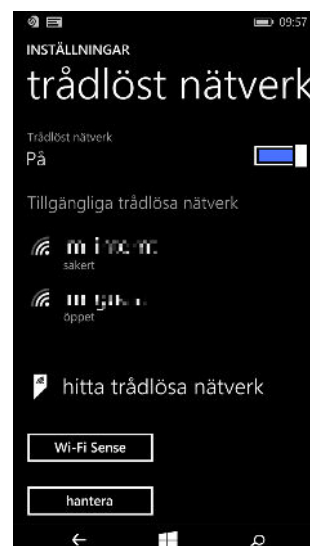
Observera också att Windows Phone har en funktion som kallas för *Wifi Sense*. Det är en funktion som ska göra det enklare att hitta trådlösa nätverk att koppla upp sig till: De nätverk som du har inloggningsuppgifter till kan du automatiskt dela med dig av till dina vänner, i utbyte mot "deras" trådlösa nät. Ur ett källskyddshänseende är det dock problematiskt, eftersom du inte vet vilka nät din telefon (eller dator, om du använder Windows 10) kommer att koppla upp sig till. Därför är det en bra idé att se till att funktionen är avstängd.



6

Välj krypterade nät

I listan med trådlösa nätverk som finns i närheten visar texten *Säkert* under nätverksnamnet att det är ett krypterat nät. Välj alltid att koppla upp till krypterade nätverk. I ett nätverk som inte är krypterat ökar risken för att någon avlyssnar datatrafiken.



7

Använd VPN

Om du har tillgång till en VPN-tjänst som använder tekniken IPsec kan du koppla upp din telefon till den.

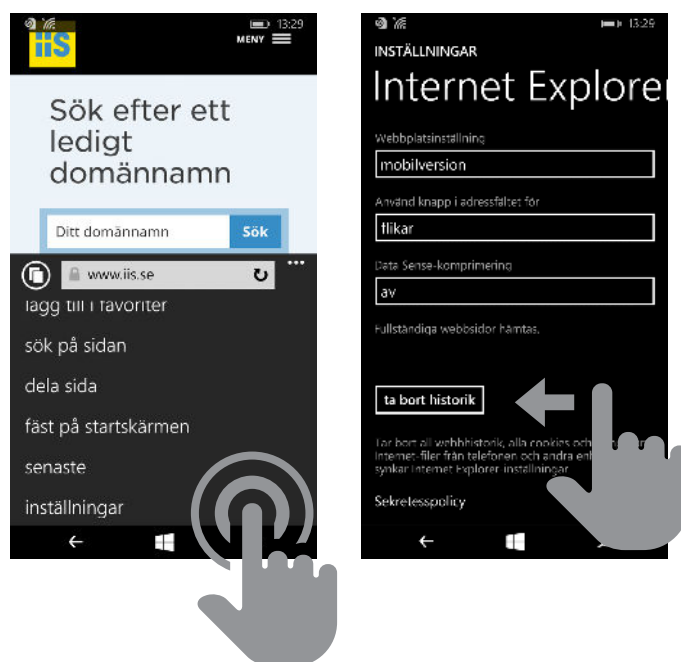
Klicka på *VPN* under *Nätverk + trådlöst*. Klicka sedan på plus-knappen för att lägga till dina inloggningsuppgifter till VPN-tjänsten.

8

Rensa surfhistoriken

I webbläsaren Internet Explorer, klickar du på de tre prickarna i nedre högra hörnet. Välj *Inställningar*. Välj *Ta bort historik*.

Använder du en annan webbläsare än Internet Explorer finns motsvarande funktion för att rensa i surfhistoriken.



9

Krypterad surf

När du använder webbläsaren, välj om möjligt adresser som börjar med HTTPS i stället för HTTP. Överföringar via HTTPS är skyddade med kryptering och försvårar därför för den som vill försöka avlyssna din webbtrafik.

Att förbindelsen till webbservern är krypterad indikeras av en ikon i form av ett hänglås i webbläsarens adressfält.



10

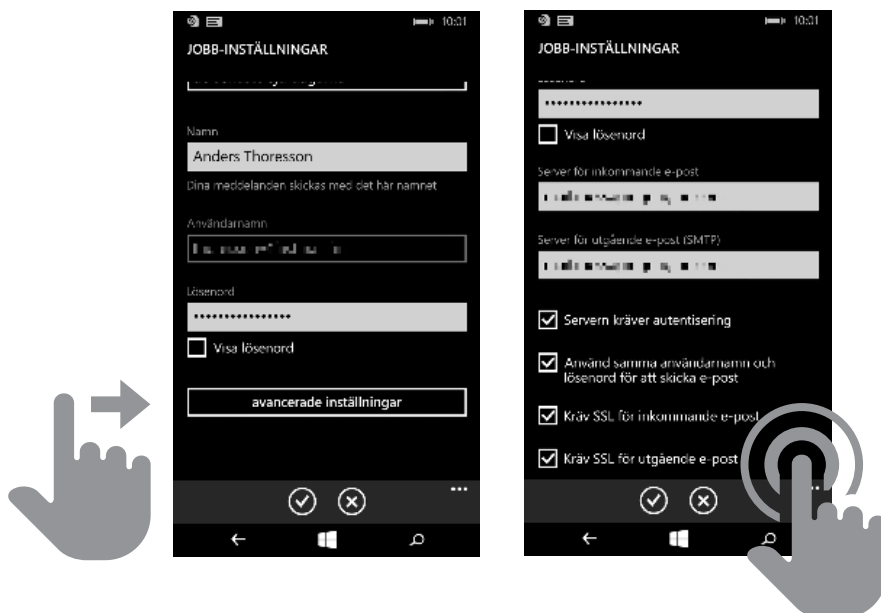
Krypterad e-post

Om du använder telefonens e-postprogram är det en bra idé att se till att mejlen hämtas och skickas via en krypterad förbindelse.

I *Inställningar*, välj *E-post + konton*. Välj det konto du vill ändra inställningarna för.



Välj *Avancerade inställningar* längst ner. Aktivera *Kräv SSL för inkommande post* och *Kräv SSL för utgående post*.



11

Positionering – slå av gps-funktionen

För att hindra alla appar i telefonen från att använda positioneringstjänster, välj *Position* i *Inställningar*. Stäng av *Positioneringstjänster*.



12

Positionering - vanliga platser

Längst ned i *Inställningar* finns alternativet *Rörelsedata*. Här kan du välja om telefonen ska logga de platser du ofta besöker eller inte.



Lär dig mer



Lär dig digitalt självförsvar!

Det innehåll som du just läst hör ihop med Internetguiden ”Digitalt självförsvar – en introduktion”. Guiden är framtagen i samarbete med Journalistförbundet och kan vara till stor hjälp för privatpersoner om de vill tipsa medier på säkrare sätt. Reportrar Utan Gränsers Martin Edström och Carl Fridh Kleberg från Expressen ger dig hjälp att med enkla verktyg skydda dig mot de hot som finns mot allas vår kommunikation och information på nätet. Innehållet vänder sig i första hand till människor som har information de vill ska komma ut till allmänheten, tipsare och uppgiftslämnare. Här finns också mycket att hämta om du vill börja kommunicera på säkrare sätt eller helt enkelt vill veta lite mer om hur internet fungerar. Författarna tar även upp sådant som massövervakning och de spår du lämnar efter dig på internet.

Fotnoter

1. Mobilen spårar dig – överallt, artikel i Dagens Nyheter – <http://www.dn.se/ekonomi/mobilen-sparar-dig-overallt/>
2. Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, artikel i The Guardian – <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-agry-birds-personal-data>
3. Så lätt är det att kapa ditt företag, artikel i Svenska Dagbladet – http://www.svd.se/sa-latt-ar-det-att-kapa-ditt-foretag_7955164
4. Mer om Tor kan du läsa i Internetguiden *Kom igång med Tor!*
5. Mer om PGP och hjälp att komma igång finns i Internetguiden *Kom igång med PGP!*
6. Hemliga data kvar i mobilen, artikel i Computer Sweden – <http://computersweden.idg.se/2.2683/1.485819>

Anders Thoresson

Anders Thoresson är journalist och föreläsare. Han har bevakat teknikutvecklingen sedan 1999. Först på tidningen Ny Teknik och sedan 2006 som frilans. Under åren 2011-2014 skrev han Teknikbloggen på dn.se. Han föreläser i samma ämnen, bland annat om digitalt källskydd för journalister och programmering i skolan för lärare och skolledare. Anders Thoresson har författat flera Internetguider för IIS, exempelvis om programmering för barn, it-säkerhet, webbpublicering och omvärldsbevakning.



Foto: Sebastian LaMotte CC-BY ND

Säkrare mobiltelefon

IIS Internetguide #38

Version 1.0 2016

Texten skyddas enligt lag om upphovsrätt och tillhandahålls med licensen Creative Commons Erkännande 2.5 Sverige.



Illustrationerna skyddas enligt lag om upphovsrätt och tillhandahålls med licensen Creative Commons Erkännande-Icke-Kommersiell-IngaBearbetningar 2.5 Sverige.



Läs mer om ovanstående villkor på <http://www.creativecommons.se/om-cc/licenserna/>

Vid bearbetning av verket ska IIS logotyper och IIS grafiska element avlägsnas från den bearbetade versionen. De skyddas enligt lag och omfattas inte av Creative Commons-licensen enligt ovan.

IIS klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission.

Författare: Anders Thoresson

Redaktör: Hasse Nilsson

Projektledare: Jessica Bäck

Formgivning: AGoodId

ISBN: 978-91-7611-450-6

Vi driver internet framåt! IIS arbetar aktivt för positiv tillväxt av internet i Sverige. Det gör vi bland annat via projekt som samtliga driver utvecklingen framåt och gynnar internetanvändandet för alla. Exempel på pågående projekt är:

Bredbandskollen

Sveriges enda oberoende konsumenttjänst för kontroll av bredbandsuppkoppling. Med den kan du på ett enkelt sätt testa din bredbandshastighet.
www.bredbandskollen.se

Internetdagarna

Varje höst anordnar vi Internetdagarna som är Sveriges ledande evenemang inom sitt område. Vad som för tio år sedan var ett forum för tekniker har med åren utvecklats till att omfatta samhällsfrågor och utvecklingen av innehållet på internet. www.internetdagarna.se

Internetfonden

Hos Internetfonden kan du ansöka om finansiering för fristående projekt som främjar internetutvecklingen i Sverige. Varje år genomförs två allmänna utlysningar, en i januari och en i augusti. www.internetfonden.se

Internetguider

IIS publicerar kostnadsfria guider inom en rad internetrelaterade ämnesområden, som webb, pdf eller i tryckt format och ibland med extra-material.

Internetstatistik

Vi tar fram den årliga, stora rapporten "Svenskarna och internet" om svenskarnas användning av internet och dessemellan ett antal mindre studier.

Webbstjärnan

Webbstjärnan är en skoltävling som ger pedagoger och elever i den svenska grund- och gymnasieskolan möjlighet att publicera sitt skolarbete på webben. www.webbstjarnan.se

Internetmuseum

I december 2014 lanserade IIS Sveriges första digitala internetmuseum. Internetmuseums besökare får följa med på en resa genom den svenska internethistorien.
www.internetmuseum.se

Federationer

En identitetsfederation är en lösning på konto- och lösenords-hanteringen till exempel inom skolans värld eller i vården. IIS är federationsoperatör för Skolfederation för skolan och för Sambiförvård och omsorg.
www.iis.se/federation

Internets infrastruktur

IIS verkar på olika sätt för att internets infrastruktur ska vara säker, stabil och skalbar för att på bästa sätt gynna användarna, bland annat genom att driva på införandet av IPv6. www.iis.se

Sajtkollen

Sajtkollen är ett verktyg som enkelt låter dig testa prestandan på en webbsida. Resultatet sammanställs i en lättbegriplig rapport.
www.sajtkollen.se

Läs mer på nätet redan idag! På Internetguidernas webbplats hittar du mängder av kostnadsfria publikationer. Du kan läsa dem direkt på webben eller ladda ner pdf-versioner. Det finns guider för dig som vill lära dig mer om webbpublicering, omvärldsbevakning, it-säkerhet, nätets infrastruktur, källkritik, användaravtal, barn och unga på internet, digitalt källskydd och mycket mer.

Nya Internetguider!



Ungas integritet på nätet

Råd till dig som är vuxen

Av: Åsa Secher

Den här guiden belyser vad integritet på nätet betyder för unga idag. Det är ett viktigt ämne att ta sig an för att vi som vuxna ska kunna stötta och hjälpa barn och unga att känna var deras gränser går så att de inte råkar illa ut. Guiden riktar sig till vuxna i barns närhet och även om internetanvändandet börjar i tidig ålder, handlar innehållet framför allt om unga i åldrarna 10 till 16 år. Du får bland annat ta del av vad unga gör på nätet, vad grooming är, hur du som vuxen kan hjälpa unga att sätta gränser och vad Barnkonventionen säger om ungas rätt till integritet. Guiden är producerad i samarbete med Barnens Rätt i Samhället (BRIS).



Skydda dig mot bedragare

Nätfiffel, bluffakturor och vilseledande försäljning

Av: Anders Nyman

Internet och telefoni skapar fantastiska möjligheter för köpare och säljare att interagera. Den här guiden handlar om myntets baksida, bedragarna som utnyttjar nätets möjligheter för att lura dig för deras egen vinning. I guiden tar vi upp bedragarnas metoder, vad du som privatperson kan råka ut för och vad du bör se upp med. Viktigast av allt: du får reda på dina rättigheter och hur du skyddar dig om du blivit lurad. Ta del av drabbades berättelser och gå igenom checklistorna så att du blir säkrare när du använder internet för att köpa produkter och tjänster i vardagen. Guiden är producerad i samarbete med Polisen.