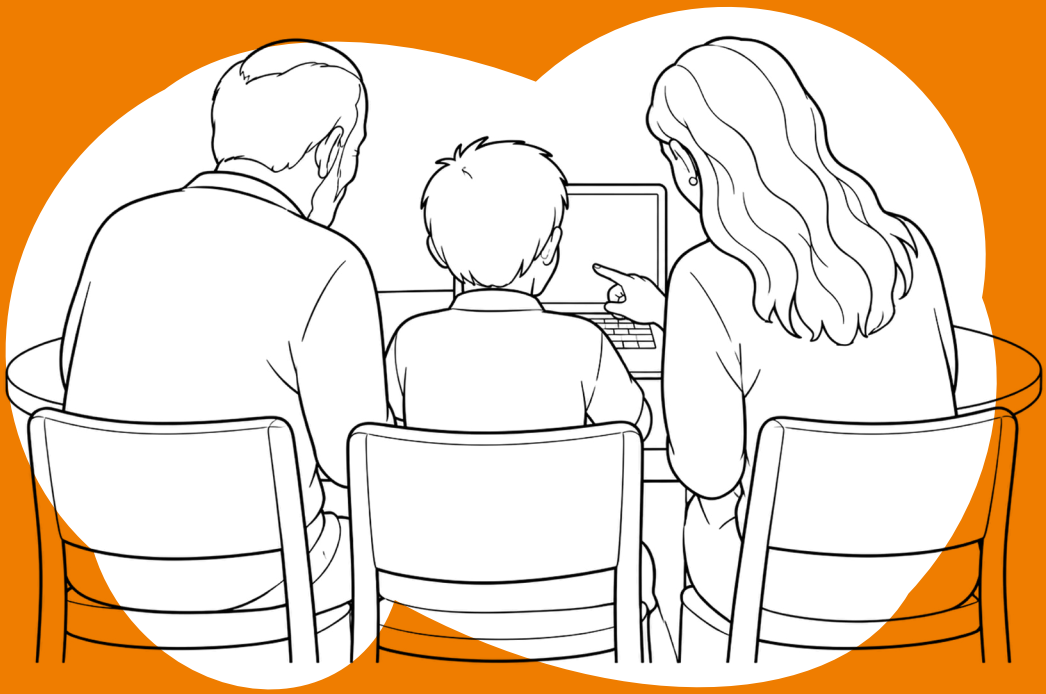


Din digitala beredskap.

En handbok i digitala hot och skydd

Den här broschyren är skapad som ett projektarbete under cybersäkerhetsstudier på Technigo. Broschyren är avsedd att fungera som en kunskapsbas och hjälpmedel för Sveriges invånare att stärka sin beredskap och motståndskraft mot digitala hot i vardagen. Informationen i broschyren är samlad från svenska myndigheter och Internetstiftelsen under september 2026.

Skapad av Linn Hasselgren

Till Sveriges invånare

Vår vardag är idag mer uppkopplad än någonsin.
Vi kommunicerar, handlar, sköter bankärenden och hanterar vårt arbete via mobiler, datorer och internet. Ofta utan att tänka på vilka risker det för med sig. Precis som fysiska kriser och konflikter kan digitala hot drabba oss alla oavsett ålder, yrke eller teknisk vana.

Sverige satsar idag stort på totalförsvaret, där både individer och civilsamhället har en central roll. Hittills har fokus främst legat på fysiska kriser och krigföring, medan kunskapen om digitala hot ofta är låg. Eftersom allt mer av vår vardag och arbete sker via digital teknik och internet är cybersäkerhet en lika viktig del av vårt gemensamma försvar.

Genom att öka din egen kunskap, medvetenhet och motståndskraft bidrar du inte bara till din egen säkerhet, utan även till ett starkare Sverige. I broschyren får du kunskap om vanliga digitala hot och konkreta råd om hur du skyddar dig själv och dina nära.

Innehåll

Checklista....6

Var står du idag....7

Nätfiske....8

Telefonbedrägeri....10

AI i bluffar....12

Skydda din information....14

Skadliga program och virus....16

Lösenord och hantering....18

Säkert internet och wifi....20

Om du är orolig....24

Mer information och fördjupning....25

Begreppsförklaring....26

Hur du använder broschyren

Broschyren är tänkt att användas som en praktisk uppslagsbok. Varje avsnitt tar upp ett specifikt digitalt hot, hur det fungerar och konkreta råd för att skydda dig. Du behöver inte läsa allt i följd, utan kan gå direkt till det ämne som känns mest relevant för dig just nu.

Målet är att du efter att ha tagit del av innehållet ska känna dig tryggare i din digitala vardag, känna igen varningstecken på bedrägerier och hot, samt veta vilka konkreta åtgärder du kan vidta. Både för att förebygga och för att kunna agera om du drabbas.

Spara broschyren.

Checklista

Med några enkla vanor minskar du risken avsevärt för att drabbas av bedrägerier, intrång eller virus.

Här är råd som gör stor skillnad för din digitala säkerhet:

- [ ] Aktivera multifaktorautentisering (MFA) på alla konton där det går.
- [ ] Uppdatera lösenord till unika och komplexa för varje tjänst.
- [ ] Använd lösenordshanterare.
- [ ] Undvik att ansluta till publika wifi, eller använd VPN.
- [ ] Uppdatera enheter, program och appar regelbundet.
- [ ] Aktivera brandvägg och antivirus på din enhet.
- [ ] Var sunt misstänksam och dubbelkolla om du är osäker.
- [ ] Var källkritisk och säkerställ med oberoende tillförlitliga källor.

Var står du idag

Ta en stund och fundera över din egen digitala vardag. Det hjälper dig se var du redan ligger bra till och vad som är värt att prioritera.

Hur känns ditt digitala liv just nu?

Otryggt ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 Mycket tryggt

Hur ligger du till inom följande?

Starka och unika lösenord	Bra	Okej	Inte än
Aktivering av multifaktorautentisering	Bra	Okej	Inte än
Uppdaterar enheter och mjukvara	Bra	Okej	Inte än
Säkert hemmanätverk	Bra	Okej	Inte än
Källkritik och medvetenhet om bluffar	Bra	Okej	Inte än

Vilka åtgärder vill du prioritera framöver?

1.

2.

3.

Du måste inte göra allt på en gång, små steg gör stor skillnad.

Nätfiske

Så fungerar nätfiske

Nätfiske (phishing) är när bedragare utger sig för att vara en person, ett företag eller en organisation du litar på. Syftet är att lura dig att klicka på en länk eller öppna en bifogad fil via ett mejl. Det är ett av de vanligaste sätten bedragare kommer åt dina personuppgifter såsom bankuppgifter och lösenord, eller sprider virus och skadlig kod för att få tillgång till konton och system. Via sms kallas det smishing.

Så lyckas bedragare

Genom att väcka känslor som stress, rädsla eller nyfikenhet vill bedragaren få dig att agera snabbt, innan du hinner kontrollera trovärdigheten. Det kan leda till att din information hamnar i fel händer, bankbedrägerier eller att konton tas över.

Vanligast är att utge sig för en pålitlig avsändare och skicka ett trovärdigt mejl eller sms med något av följande:

- En länk till en falsk webbsida där du uppmanas att logga in eller fylla i kontouppgifter.
- Bifogad fil som du uppmanas att öppna eller ladda ner som sprider virus eller skadliga program.

Nätfiske bygger ofta på spoofing, en teknik som förfalskar avsändaradressen i ett mejl så att det ser ut att komma från någon annan än den verkliga avsändaren. På så sätt kan det se ut som att det är din bank, ditt barn eller ett företag som kontaktat dig, trots att så inte är fallet.

Mejlhanterare fångar upp en del misstänkta mejl automatiskt, men bedragare blir allt skickligare och ditt eget omdöme är det bästa skyddet.

Så här kan du skydda dig

- Klicka aldrig på en länk eller fil utan att dubbelkolla legitimiteten.
- Lita aldrig på avsändarnamnet eller logotyper. De är enkla att förfalska.
- Gå själv till avsändarens officiella webbplats istället för att följa länken.
- Lämna aldrig ut kortuppgifter, koder eller lösenord.
- Kom överens om ett kodord eller kontrollfrågor med nära anhöriga för att säkerställa att du pratar med rätt person.
- Radera tvivelaktiga mejl.

Tänk efter: väntade du dig det här meddelandet?
Har du inte beställt något, bett om en lösenordsåterställning eller har någon relation till avsändaren, är det troligen en bluff.

Om du blivit drabbad

- Kontakta din bank om du lämnat ut kortuppgifter eller inloggat in med e-legitimation.
- Polisanmäl vid brott.
- Byt lösenord eller kod till berörda konton.



Telefonbedrägeri

Så fungerar vishing

Vishing (voice + phishing) är telefonbedrägeri där skickliga bedragare använder röst och retorik för att skapa falsk brådska eller oro och få dig att agera utan att tänka efter. Bedragarna låter empatiska och står på sig, vilket gör dem svåra att stå emot.

Målet kan vara att:

- Lura dig till att avslöja personlig information.
- Uppge kort- eller kontouppgifter.
- Använda din e-legitimation.
- Utföra ekonomiska transaktioner.
- Få dig att ladda ner en app eller ett program.

Så lyckas bedragare

Bedragare har ofta tagit reda på information om dig som är publikt tillgänglig såsom din adress, anhöriga eller om du är med i en förening som bevis för att de är den person eller organisation de utger sig för att vara.

Det är enkelt för bedragare att förfalska telefonnumret som de hör av sig ifrån genom tekniken spoofing. Det är en metod som används av bedragare när man på teknisk väg lurar mottagaren till att tro att samtalet eller sms:et kommer från en betrodd avsändare. På så sätt kan det se ut som att det är din bank, ditt barn eller ett företag som ringer eller skickat ett sms, trots att så inte är fallet.

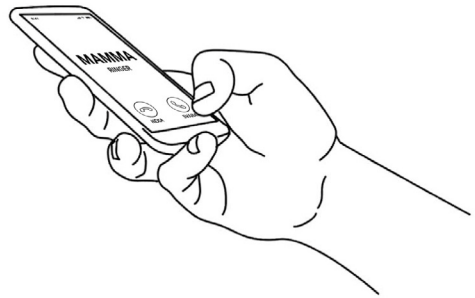
Lyssna på magkänslan. Låter personen annorlunda, agerar konstigt jämfört med hur din närstående brukar vara, eller sätter dig i en obekväm sits? Du behöver inte vara trevlig och kan lägga på samtalet direkt.

Så här kan du skydda dig

- Ring alltid tillbaka på ett nummer du själv sökt fram och aldrig på det numret som ringde dig.
- Logga aldrig in på bank eller konton under ett samtal.
- Lämna inte ut kontouppgifter, koder eller lösenord.
- Lita inte på uppringaren bara för att hen vet saker om dig.
- Kom överens om ett kodord eller kontrollfrågor med nära anhöriga för att säkerställa att du pratar med rätt person.
- Är du osäker? Avsluta samtalet direkt.
- Blockera misstänkta nummer.

Om du blivit drabbad

- Kontakta din bank om du lämnat ut kortuppgifter eller inloggat in med e-legitimation.
- Polisanmäl vid brott.
- Byt lösenord eller kod till berörda konton.



AI i bluffar

AI och samhällsutveckling

Artificiell intelligens (AI) utvecklas i snabb takt och får en allt större betydelse för samhällsutvecklingen. Tekniken påverkar hur företag och organisationer arbetar, hur tjänster produceras och hur människor lever och kommunicerar. Generativ AI är den typ av AI som vi använder mest i vardagen (t.ex. ChatGPT, Claude, eller Gemini). Det kan effektivisera uppgifter och generera nytt innehåll men utnyttjas även av bedragare för att öka legitimiteten i bluffar. Bästa skyddet är kunskap om teknikens möjligheter.

Deepfakes

Deepfakes är övertygande förfalskningar i form av video eller ljud skapade av ett datorprogram. Deepfakes kan vara underhållande men också användas för att sprida desinformation eller utföra bedrägerier. Det är vanligt att kändisar och politiker utsätts i störst utsträckning men även privatpersoner kan drabbas.

Röstkloning

Bedragare kan klona röster med hjälp av AI för att få dig att tro att du pratar med någon du litar på eller är beroende av. Syftet kan vara att lura dig att göra en transaktion, uppge inloggningsuppgifter eller investera pengar. Exempelvis genom en förfalskad röst från ditt barn i en påhittad krissituation eller en anställd på din bank som uppger att de behöver ditt godkännande via e-legitimation. Historier kan variera men bedragaren spelar på känslor och påhittade krissituationer för att du ska agera snabbt utan att kontrollera.

Det krävs bara några sekunders inspelning av en röst för att skapa en trovärdig röstklon.

Falska videor

Falska videor är numera lätta att skapa och kan se helt äkta ut. Avsikten kan vara att luras genom att visa en person, eller påhittad situation. Falska videor används ofta för desinformation, investeringsbedrägerier eller för att få dig att lämna ut personlig information. Det är lätt att bli lurad då filmat material ofta uppfattas som bevis på att något har skett.

Trovärdiga bedrägerier

Bedragare kombinerar deepfakes med webbplatser som ser legitima ut, falska omdömen och trovärdig kommunikation. Tidigare kunde språkfel eller avvikelser i videor avslöja bluffar men utvecklingen av AI gör numera språket och mänskliga uttryck nästan felfritt.

Med kunskap, eftertanke och källkritik minskar du risken för att bli lurad.

Så här kan du skydda dig

- Var medveten om tekniken. Vetskapen om förfalskningar gör dig bättre rustad att upptäcka en bluff.
- Var källkritisk. Var extra uppmärksam på innehåll som väcker starka känslor, och dela bara information som kommer från pålitliga källor.
- Lämna inte ut kontouppgifter, koder eller lösenord.
- Var misstänksam om du uppmanas att agera direkt. Bedragare utnyttjar tidspress och känslor för att du inte ska hinna tänka efter.
- Kom överens om ett kodord eller kontrollfrågor med nära anhöriga för att säkerställa att du pratar med rätt person.

Skydda din information

Vad är privat information

Din mobil, surfplatta och dator innehåller mycket privat information om dig och dina närstående. Därför är det viktigt att vara rädd om dessa saker och skydda informationen som finns där.
Det kan exempelvis vara:

- Bilder och filmer
- Chattar och meddelanden
- Platsinformation
- Inloggningar till konton
- Information om vänner och anhöriga
- Uppgifter om din hälsa

Var medveten om vilken information du delar till exempel när du laddar ner en ny app, skapar ett konto, skriver med en AI eller delar platsinformation via tjänster. Överväg alias istället för namn, stäng av platsdelning vid behov och ta reda på vad appar sparar om dig.

Dataintrång

Dataintrång är olagligt och innebär att någon utan tillstånd tar sig in i ett datorsystem där data och information behandlas, lagras eller överförs elektroniskt. Syftet är vanligtvis att orsaka skada genom att blockera tjänster, stjäla eller förstöra information, eller kryptera information i utpressningssyfte. Företag drabbas oftast av mer komplexa intrång, medan privatpersoner utsätts för enklare intrång men som ändå påverkar vardagen kraftigt. För privatpersoner kan det vara att någon tar sig in i din dator utan lov eller tar över ett sociala medier-konto. Målet är i nästan alla fall att stjäla information eller utpressning på pengar.

Hur tar man över ett konto

Konton kapas oftast på grund av svaga lösenord eller att du använder samma inloggningsuppgifter på flera ställen. Angripare kan snabbt testa tusentals slumpmässiga lösenord på mycket kort tid och lyckas med en inloggning. Uppgifter kan även läcka vid intrång hos tjänster du använder som senare används för att kapa konton.

Så här kan du skydda dig

- Använd starka och unika lösenord till alla konton.
- Aktivera multifaktorautentisering där det är möjligt.
- Gå igenom dina konton med jämna mellanrum och radera de du inte längre använder.

Om du blivit drabbad

- Kontakta plattformens utgivare för hjälp att återfå kontot.
- Byt lösenord på andra tjänster där du använt samma uppgifter.
- Vid meddelande om intrång eller läckage hos en tjänst du använder är det bra om du kontrollerar vilken information tjänsten sparat om dig och byt lösenord på den tjänsten och andra konton.

Skadliga program och virus

Hur får man virus

Intrång i din enhet kan ske via skadliga program och virus, vilket kan leda till stulna kortuppgifter och lösenord, långvarig övervakning eller kryptering av filer. Utpressningsvirus (ransomware) kan låsa datorn eller kryptera filer och angriparen kräver ofta en lösensumma för att låsa upp dem.

Det kan spridas genom:

- Falska programuppdateringar
- Falska virusvarningar
- Besök på skadliga webbplatser
- E-postbilagor
- Trojaner

En trojan är något som utger sig för att vara något annat än vad det egentligen är. Det kan dölja sig bakom vad som helst på internet, till exempel bilder, filmer, länkar eller programvaror och det kan räcka med att du öppnar en bild eller fil för att bli infekterad med virus.

Betala aldrig en lösensumma vid utpressningsvirus. Det finns ingen garanti för att du får tillbaka din information eller konton även om du betalar.



Så här kan du skydda dig

- Klicka inte på länkar, annonser, bilagor eller öppna bilder utan att först kontrollera att de går att lita på.
- Ladda bara ner program från officiella och pålitliga källor.
- Använd aldrig okända USB-minnen, endast från betrodda källor.
- Använd antivirusprogram och aktivera brandväggen på datorn. Antivirus upptäcker och blockerar skadliga nedladdningar.
- Uppdatera programvaror. Virus sprids ofta via svagheter i webbläsare, operativsystem och mjukvara och uppdateringar åtgärdar dessa.
- Ta regelbundna säkerhetskopior av dator, mobil och surfplatta. Spara det på till exempel USB-minne, hårddisk eller i molntjänst. Testa då och då att kopian går att återställa.

Om du blivit drabbad

- Agera direkt. Koppla bort enheten från internet.
- Gör en fullständig genomsökning med antivirusprogrammet.
- I värsta fall kan en fabriksåterställning krävas. Då återställer man en enhet till sitt ursprungliga skick, vilket raderar all data och alla program.
- Byt lösenord på dina viktigaste konton (mejl, sociala medier osv.) från en annan enhet.
- Kontakta banken för att eventuellt spärra kort och håll uppsikt på misstänkt aktivitet.
- Polisanmäl vid brott.

Lösenord och hantering

Varför lösenord är viktiga att skydda

De flesta tjänster kräver en personlig inloggning med användarnamn eller mejladress och lösenord för att skapa ett konto. I många tjänster lagras vanligtvis personlig information och det är därför viktigt att skydda inloggningsuppgifter från obehöriga.

Din privata e-post är extra viktig att skydda, då den oftast fungerar som ”huvudnyckel” och kan användas för att återställa lösenord till dina andra konton. Utöver att vi själva kan läcka lösenord kan även webbplatser vi registrerat oss på drabbas av intrång eller läckor.

Angripare använder lätt gissade lösenord eller läckta lösenord från hackade tjänster för att testa om du återanvänt dem. Du bör därför välja starka lösenord: långa, ovanliga, opersonliga och unika.

Hantering av svåra lösenord

Att spara lösenord i webbläsaren kan vara enkelt och är vanligtvis något som erbjuds via en popup-ruta. Det är användarvänligt men inte alltid säkert. Blir enheten stulen eller utlånad får obehöriga direkt tillgång.

En lösenordshanterare är en app eller ett tillägg i webbläsaren som skapar och sparar långa, unika lösenord åt dig på ett säkrare sätt. På så vis kan du använda långa lösenord utan att behöva komma ihåg dem själv. Det finns många olika lösenordshanterare på marknaden så undersök noga vilken som passar dig bäst.



Multifaktorautentisering (MFA)

Även om du använder långa och unika lösenord är det fortfarande inte ett tillräckligt skydd på dina viktigaste konton. MFA innebär att du bekräftar din identitet med mer än bara lösenordet. Det är till exempel genom en kod som skickas till mobilen, en app eller fingeravtryck/ansiktsigenkänning. Det gör det betydligt svårare för en angripare att komma åt ditt konto även om de skulle komma över ditt lösenord. MFA aktiveras på varje separat konto eller inloggning och inte som en inställning på din enhet.

Tips på hur du skapar starka lösenord och skyddar konton

- Använd inte enkla lösenord som ”12345”, ”password” eller ”qwerty”.
- Gör lösenordet långt, det är viktigare än att det är krångligt. Sätt gärna ihop flera slumpmässiga ord till en fras.
- Använd aldrig samma lösenord på flera konton.
- Logga inte in på viktiga konton på andras enheter då de kan spara lösenord eller vara infekterade med skadlig kod.
- Aktivera alltid multifaktorautentisering (MFA) där det är möjligt, speciellt till dina viktigaste konton.
- Använd en lösenordshanterare som skapar och sparar långa och unika lösenord åt dig.

Du kan kolla om ditt lösenord, e-postadress eller andra personuppgifter finns med i en databasläcka. Besök internetstiftelsens hemsida, internetkunskap.se/har-mitt-losenord-lackt.

Säkert internet och wifi

Hur fungerar wifi

Wifi är den vanligaste tekniken för trådlösa nätverk och gör att enheter kan koppla upp mot internet utan kabel. När wifi-funktionen är påslagen sänder din enhet information via radiovågor inom en begränsad räckvidd för att kunna hitta och ansluta till nätverk.

Kryptering

För att skydda information som skickas mellan din enhet och en webbplats krypteras antingen informationen, förbindelsen eller båda. Kryptering innebär att information eller internettrafik omvandlas till en oläsbar kod som bara kan tolkas av den som har rätt nyckel för att låsa upp den. Vid vanlig webbsurfning räcker oftast en krypterad förbindelse. Ett hänglås vid adressfältet och att adressen börjar med ”https” (S för ”secure”), visar att förbindelsen är skyddad. De flesta webbplatser vi besöker idag har en krypterad förbindelse.

Virtual Private Network (VPN)

En VPN-tjänst är en app eller programvara du ansluter till, som krypterar din internettrafik och döljer din information från utomstående när du surfar. Den skapar en osynlig tunnel mellan din enhet och internet och är extra användbar på osäkra nätverk såsom publikt wifi. Det finns många olika VPN-tjänster på marknaden så undersök noga vilken som passar dig bäst.



Surfa på publikt wifi

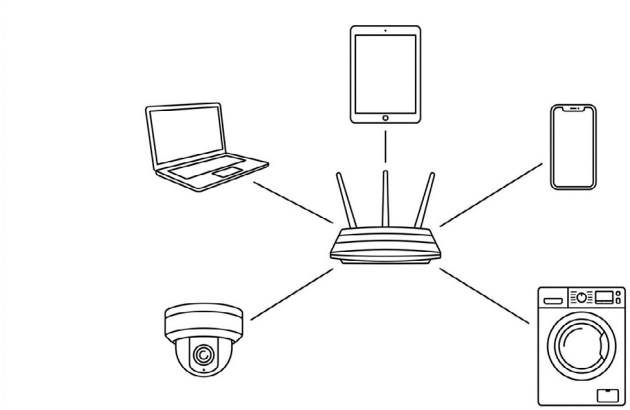
När du kopplar upp dig på ett publikt nätverk ökar risken att någon obehörig kan ta del av din information. Publika nätverk som till exempel på caféer, flygplatser, hotell eller bibliotek saknar ofta kryptering, vilket gör att andra i närheten kan ta del av din information. Många publika nätverk kräver inte inloggning eller tillåter att användare delar samma lösenord. Angripare skapar också enkelt nätverk med falska namn för att lura dig att koppla upp dig mot deras wifi istället för till exempel caféets riktiga wifi.

Surfa via mobiloperatörens nätverk

Att surfa via 4G/5G innebär att din telefon ansluter till internet genom mobiloperatörens nätverk istället för wifi. Förbindelsen är krypterad och därför betydligt säkrare än ett oskyddat publikt wifi-nätverk.

Surfa säkert på publika wifi

- Undvik publika wifi och koppla hellre upp datorn mot mobilen.
- Se upp för falska nätverk. Lita bara på kända namn, och var extra aktsam om flera snarlika namn finns som publika nätverk.
- Stäng av wifi när det inte används. Det minskar risken för oönskad uppkoppling och sparar batteri.
- Rensa bort gamla wifi-nätverk som du kopplat upp dig på tidigare och behåll endast de du känner till och litar på.
- Besök bara krypterade sidor. Kontrollera hänglåset och ”https” innan du anger inloggningsuppgifter.
- Använd VPN som krypterar din trafik.



Skydda ditt hemmanätverk

De flesta har en router hemma som kopplar upp digitala enheter mot internet. Routern fungerar som länken mellan ditt hemmanätverk och internet. Genom att skydda routern blir det svårare för obehöriga att använda ditt trådlösa nätverk, spionera på dig, missbruka din uppkoppling för illegala syften eller stänga ute dig från ditt eget nätverk.

Smarta enheter i hemmet

Smarta enheter såsom hemlarm, robotgräsklippare, belysning eller tvättmaskin kopplas ofta upp mot internet via wifi för att kunna styras och övervakas på distans. Många tillverkas i andra länder vilket kan innebära en risk om säkerheten i produkten inte håller tillräckligt hög standard. Blir en enhet utsatt för intrång kan en angripare i värsta fall få åtkomst till ditt nätverk eller övriga anslutna enheter.

För att kunna följa råden i det här avsnittet behöver du läsa din routers instruktionsmanual. Du kan oftast hitta manualen på webben genom att söka på ”märke, modell och +manual”.

Gör ditt hemmanätverk säkrare

- Byt standardlösenordet till administratörskonton. Förinställda uppgifter är till för att installationen ska gå smidigt men är lätta för angripare att komma över. Byt användarnamn och lösenord direkt efter installation.
- Byt namn och lösenord på ditt wifi. Nätverksnamnet avslöjar ofta routerns tillverkare och modell och bör därför bytas ut efter installation. Använd inte namn som avslöjar personlig information om dig.
- Uppdatera mjukvaran i routern regelbundet och aktivera automatiska uppdateringar om möjligt. Uppdateringar åtgärdar svagheter och fel samt lägger till nya funktioner.
- Använd stark kryptering i router. De flesta routrar erbjuder olika krypteringsstandarder som är olika svåra att knäcka. WPA3 är den senaste och starkaste standarden men du kan välja WPA2 om dina enheter inte stödjer den senaste. Stödjer routern varken WPA2 eller WPA3 bör den bytas ut.
- Stäng av WPS och UPnP i router. Dessa funktioner underlättar installation men är aktiverade som standard och kan utgöra säkerhetsrisker. Stäng av eller begränsa dem.
- Dela upp ditt nätverk via routern. Du kan dela upp hemmanätverk i flera separata delar till exempel genom att skapa ett gästnätverk med eget namn och lösenord. Det är som att skapa flera osynliga rum inom nätverket som inte kan nå varandra. Det gör det svårare för en angripare att komma åt ditt vanliga nätverk där din telefon, dator eller surfplatta är anslutna. Då kan gäster surfa på internet utan att komma åt dina andra enheter. Det är också bra att koppla upp smarta enheter såsom hemlarm eller robotgräsklippare på gästnätverket eller en helt egen del.

Känns något för avancerat kan du fråga en kunnig bekant, familjemedlem eller din bredbandsoperatör om hjälp.

Om du är orolig

Digitaliseringen går snabbt och samhället förändras i en allt högre takt. Nya tjänster, tekniker och risker tillkommer ständigt vilket gör det svårt att alltid hänga med och känna sig trygg.

- Har du blivit utsatt för ett brott, gör alltid en polisanmälan. Du kan anmäla via polisen.se eller genom att ringa 114 14, eller 112 om det är ett akut nödläge.
- Känner du oro eller behöver någon att prata med efter att ha blivit utsatt för brott kan du vända dig till Brottsoffermyndigheten för stöd och information om dina rättigheter.

Prata med anhöriga eller vänner om du känner dig orolig. Be om hjälp om något av rekommendationerna i broschyren känns svårt att förstå eller genomföra. Det är bättre att fråga och prata med varandra än att stå ensam med osäkerheten.



Mer information och fördjupning

Cybersäkerhet är ett stort område och i broschyren har de flesta aktuella råden samlats men det finns mer att läsa om du vill fördjupa dina kunskaper ytterligare. All information i broschyren är samlad från dessa källor under september 2026.

Polisen.se
Krisinformation.se
Integritetsskyddsmyndigheten.se
Ncsc.se
Internetstiftelsen.se

Begreppsförklaring

Angripare: någon som utför en attack eller ett bedrägeri mot din enhet eller ditt nätverk.

Applikation (app): ett program som du laddar ner på din enhet för att utföra en viss uppgift.

Artificiell intelligens (AI): datorprogram som är tränade på stora mängder information för att känna igen mönster och utföra uppgifter.

Administratörskonto: ett konto som ger dig full kontroll över en enhets alla inställningar.

Brandvägg: ett skydd som övervakar och blockerar oönskad trafik mellan din enhet och internet.

Cybersäkerhet: arbetet med att skydda digitala enheter, nätverk och information från digitala hot och intrång.

E-legitimation: en digital Id-handling som används för att bevisa vem du är och logga in på tjänster (t.ex. BankID, Freja eID eller Sverige-id).

Enhet: samlingsord för tekniska prylar som mobil, dator, surfplatta eller smarta prylar som du kopplar upp mot internet.

Generativ AI: en typ av artificiell intelligens som kan skapa nytt innehåll som text, bilder, röster eller video baserat på stor mängd inlärd information.

Intrång: När någon obehörig tar sig in i ett konto, en enhet eller ett nätverk.

Identitet (digital): de uppgifter och inloggningar som representerar vem du är på internet (t.ex. användarnamn och kontouppgifter).

Kryptering: att omvandla information till en hemlig kod som bara kan läsas av den som har rätt ”nyckel”.

Källkritik: att granska och ifrågasätta vart informationen kommer ifrån innan man litar på den.

Molntjänst: en tjänst där du lagrar filer, bilder eller data på internet istället för direkt på din egen enhet (t.ex. Google Drive eller iCloud).

Mejlhanterare: tjänsten du använder för att läsa och skicka mejl (t.ex. Gmail eller Outlook).

Mjukvara: det samlade namnet för programmen på din enhet.

Operativsystem: grundprogrammet som får mobilen eller datorn att fungera (t.ex. Windows, iOS eller Android).

Platsinformation: uppgifter om var din enhet befinner sig geografiskt.

Säkerhetskopia (backup): en extra kopia av dina filer som sparas separat så att du kan återställa dem om originalet skulle förstöras eller försvinna.

Standardlösenord: det förinställda lösenord som en enhet eller program levereras med från fabriken.

Uppdatering: en förbättring av ett program eller operativsystem som bland annat åtgärdar kända svagheter.

Universal Plug and Play (UPnP): en funktion på routrar som låter enheter i nätverket automatiskt hitta och koppla upp sig mot varandra utan manuellt godkännande.

Wi-Fi Protected Setup (WPS): en funktion på routrar som gör det enklare att koppla upp nya enheter till wifi, genom att trycka på en knapp istället för att skriva in lösenordet.

Webbläsare: programmet du använder för att surfa på internet (t.ex. Chrome eller Safari).

Din digitala beredskap.

Genom att skydda dig själv bidrar du till en tryggare vardag och en starkare motståndskraft för Sverige.

Läs mer på hemsidan
dindigitalaberedskap.se

Kontakta mig
kontakt@dindigitalaberedskap.se

Skapad av Linn Hasselgren