Alltid online, alltid sårbar

Om digitalt våld i ungas relationer

ctrl

ATT HA DEN ÄR LIKA VIKTIGT SOM ATT SLÄPPA DEN

Förord

Kontroll är ett ord med två ansikten – en dualitet som genomsyrar våra relationer, vår självbild och vårt digitala liv. I en värld där tekniken erbjuder obegränsade möjligheter att övervaka och påverka varandra, måste vi ständigt omvärdera vad som är rimligt och respektfullt.

För unga, som navigerar i en komplex tid präglad av snabb teknisk utveckling, kan osäkerheten kring vad som är rätt och fel kännas överväldigande. Jakten på kontroll och bekräftelse kan skapa obehagskänslor och inre konflikter; en slags "glitch" i magen.

Projektet CTRL är ett samarbete mellan Fredens Hus, Uppsala Kvinnojour och Sentor med stöd av Jämställdhetsmyndigheten, och syftar till att belysa och motverka digitalt våld i ungas parrelationer. Vi vill hjälpa unga att navigera och hitta rätt, att finna den nödvändiga kontrollen i sitt eget liv, men också att stå ut med att inte ha den över andra, stå ut med allt det vi inte kan eller bör kontrollera.

Unga efterfrågar att deras föräldrar och andra vuxna i deras närhet ska ha större insikt och förståelse för det digitala våldet. Genom ökad kunskap om vad digitalt våld är, hur det tar sig uttryck, vad man kan göra för att skydda sig mot det och hur du som förälder kan ha en dialog med ditt barn, vill vi med denna folder bidra till att minska det gap som finns mellan ungas behov och vuxnas kännedom.

Vissa ämnen, som exempelvis spel, nätmobbning och grooming, kommer inte att behandlas ingående i denna folder.

För mer information och stöd, besök gärna projektets hemsida **digitalctrl.se**.

Digitalt våld

Digital säkerhet

Vad kan jag som vuxen göra?

Digitalt våld

Ungas digitala liv

Internet, smarta telefoner och annan digital teknik har blivit en naturlig del av vår vardag och upplevs för många som både självklar och nödvändig.

Vi använder digital teknik för att upprätthålla sociala relationer, ta del av nyheter och information samt kommunicera med myndigheter eller hälso- och sjukvården. Detta gäller inte minst för unga, där internet varit en integrerad del under hela livet.

För unga spelar digital teknik en särskilt viktig roll. Forskning och studier visar att tekniken inte bara är avgörande för ungas relationer och tillgång till information, utan också en viktig del av deras utveckling och lärande. Dessutom spelar tekniken en stor roll i utvecklingen av den egna identiteten hos barn och ungdomar (Folkhälsomyndigheten, 2024).

Enligt kartläggningen Svenskarna och internet (2023) använder 99 % av barn och unga i åldern 8–19 år internet. Redan på lågstadiet använder 97 % av barnen internet, och 9 av 10 gör det varje dag. På mellanstadiet, högstadiet och gymnasiet använder alla elever internet dagligen.

Unga och sociala medier

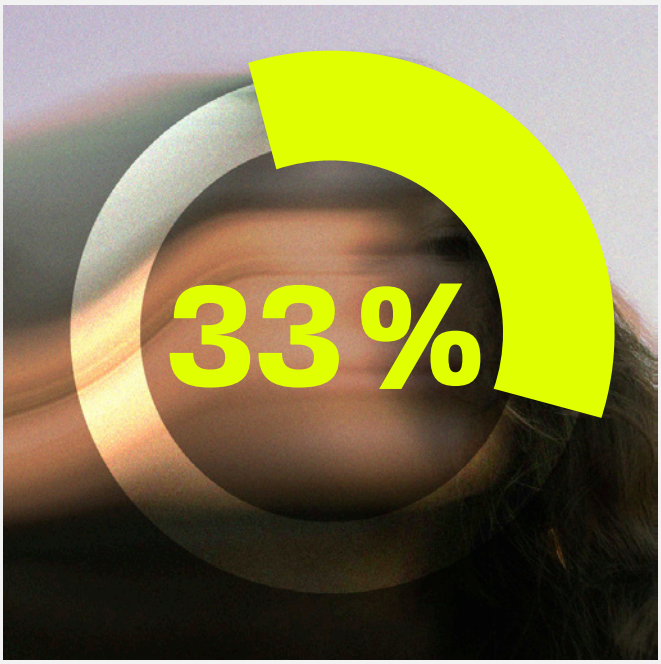
Sociala medier utgör en stor del av barn och ungas internetanvändning. 99 % av barn och unga i Sverige använder sociala medier någon gång, 97 % varje vecka och 92 % varje dag (Internetstiftelsen, 2023). Tre av fyra barn på lågstadiet använder sociala medier dagligen, och när barnen kommer upp i mellanstadieåldern och uppåt använder i princip alla sociala medier varje dag. Barn som inte använder sociala medier uppger nästan uteslutande att anledningen är att de inte får använda sociala medier för sina föräldrar (Internetstiftelsen, 2023).

Unga använder ofta sociala medier för att umgås med kompisar. Enligt Internetstiftelsen (2023) uppger ungefär hälften att detta är deras främsta drivkraft för att använda sociala medier. Barn på mellanstadiet använder främst YouTube, Snapchat, Roblox, TikTok, Instagram, Twitter, Twitch och Pinterest. YouTube är den tjänst som flest barn på mellanstadiet använder, följt av Snapchat.

Bland ungdomar på högstadiet är nästan samtliga sociala medier representerade. YouTube används mest, följt av Snapchat och därefter TikTok. TikTok har sin högsta andel användare bland ungdomar på högstadiet. På fjärde plats kommer Instagram (Internetstiftelsen, 2023).

Ny arena och nya tillfällen att utöva våld i relationer

Digital teknik har öppnat upp stora möjligheter för unga att socialisera, skapa och förstå sin egen



av alla elever i årskurs nio som dejtat/haft en relation har utsatts för någon form av våld.

(Stiftelsen Allmänna Barnhuset & Jämställdhetsmyndigheten, 2024)

identitet. Men den digitala världen har också sina baksidor. När allt mer av ungas liv flyttas till digitala platser, flyttas även våld i ungas relationer dit. Digital teknik har skapat nya arenor, metoder och tillfällen att utöva våld, och gör det möjligt för våldsutövare att väva in digital teknik i sitt våldsmönster.

Genom exempelvis sociala medier och appar kan våldsutövare övervaka och kontrollera sin partner utan att vara fysiskt närvarande. Funktioner och applikationer som skapats för att vara användarvänliga och bekväma kan missbrukas av en våldsam partner. Denna form av digitalt våld skapar nya utmaningar för oss som vuxna när vi vill skydda våra barn från att utsättas för våld i en parrelation.

Att som vuxen ha grundläggande kunskap om hur digitala enheter och dess funktioner och applikationer fungerar och kan utnyttjas, samt hur man ska agera när något inträffar, är därför avgörande för att öka säkerheten för våra barn och unga.

Vad är digitalt våld?

Det finns en mängd olika ord och benämningar för att beskriva våld som utövas med hjälp av digital teknik.

I forskningssammanhang används bland annat begreppen *technology-facilitated abuse, technology-facilitated coercive control, digital abuse* eller *digital coercive control*.

I Sverige och utanför forskningssammanhang är det vanligaste begreppet digitalt våld. Begreppet har ingen vedertagen definition, utan förklaras ofta på olika sätt beroende på vem som beskriver våldet. Vissa menar att digitalt våld är en helt ny typ av våld, medan andra hävdar att det är psykiskt våld som utövas digitalt. Det som de allra flesta är överens om är att digitalt våld handlar om våld som utövas med hjälp av digital teknik.

Vi har valt att skriva en egen definition av digitalt våld, för att skapa en bättre förståelse för vad vi menar när vi använder begreppet:

Förenklat kan definitionen beskrivas som att digitalt våld är allt våld som utförs med hjälp av digital teknik. Det kan exempelvis handla om psykiskt, sexuellt eller ekonomiskt våld. Vi menar att digitalt våld kan inkludera flera olika våldshandlingar, såsom kränkningar via samtal, sms eller sociala medier, repetitiva samtal, intrång i privata konton, spridande av känslig information och bilder, identitetsstöld eller övervakning och spårning.

Digital teknik och ungas relationer

Eftersom digital teknik spelar en särskilt viktig roll i ungas liv och vardag är det vanligt att deras relationer både upprätthålls och utvecklas via internet och sociala medier.

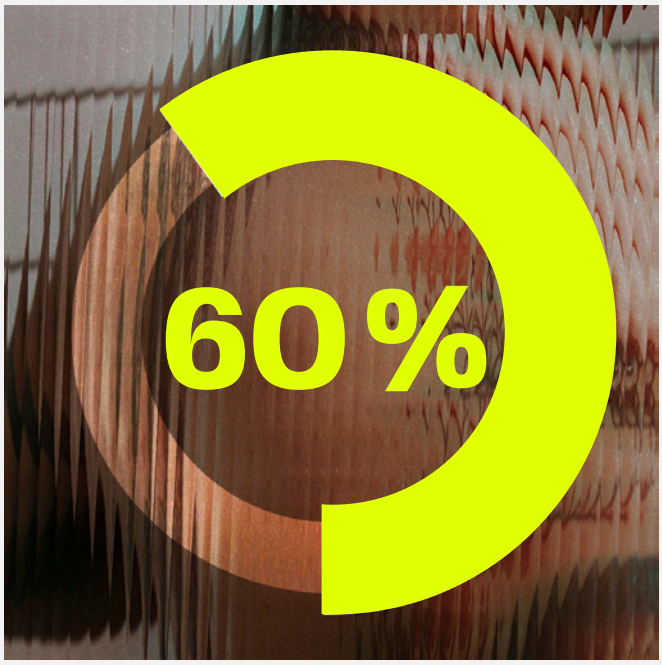
Precis som i vuxnas relationer kommer ungas parrelationer med en rad förväntningar och förutfattade tankar om hur en relation ska se ut. Bland unga är det idag inte ovanligt att partners förväntas ha tillgång till varandras telefoner och sociala medier. Detsamma gäller appar med GPS-funktioner aktiverade på telefonen för att veta var en partner befinner sig, eller att ha full insyn i vem ens partner kommunicerar med eller följer på sociala medier.

Unga plockar ofta upp dessa förväntningar från en mängd olika platser och personer utöver partners – från sociala medier, tv-serier, filmer, böcker, samt från vänner och familj. Att tillåta en partner att ha tillgång till och insyn i ens digitala liv betraktas ofta som ett tecken på tillit och förtroende, och ett bevis på att man inte döljer något. Men det är en fin linje mellan en partner som visar kärlek, tillit och omtanke genom att vara intresserad av den andres liv, och en partner som är kontrollerande och våldsam.

Linjen kan vara extra svår för unga att identifiera, som ofta saknar ordentliga referensramar kring hur en hälsosam relation ser ut. Många unga befinner sig kanske i sin första relation och har få eller inga vänner som varit i en relation tidigare som kan ge råd. I många unga relationer förekommer dessutom olika grader av tvång, där unga kan känna sig tvungna att dela med sig av exempelvis lösenord eller plats som ett bevis på trohet eller för att undvika att utsättas för våld (Korkmaz, Øverlien & Lagerlöf, 2022, Brottsförebyggande rådet, 2021).

När vi känner att vi måste göra vissa saker i en relation, finns det en risk att vi hamnar i situationer där vi gör saker som vi egentligen inte vill eller mår bra av. Det är därför viktigt att hjälpa barn och unga att reflektera över förväntningar – förväntningar på sig själv och ens partner – och att påminna om vikten att tillsammans bestämma hur relationen ska formas.

De ideal och normer som omger oss kan sätta stor press på våra relationer och påverka vad vi känner oss bekväma med att säga ja eller nej till. Att identifiera och uttrycka dessa ideal kan hjälpa oss att avgöra vilka vi vill följa och vilka vi kanske vill överge. Om vi bara agerar utifrån vad vi tror att vi "ska" göra, utan att lyssna till våra egna känslor och behov, riskerar våra relationer att formas av yttre förväntningar snarare än av våra egna val. Barn och unga kan ofta behöva stöd från vuxna i att identifiera vilka förväntningar de känner sig bekväma med.



av ungdomar i åldern 15–19 har erfarenhet av våld i nära relationer och den vanligaste formen av våld är psykiskt våld som utövas digitalt.

(Stiftelsen Allmänna Barnhuset & Jämställdhetsmyndigheten, 2024)

Förövaren i fickan

Tidigare kunde den som utsattes för våld av en partner få en viktig paus från våldet, kanske i skolan, under en fritidsaktivitet eller under kvällar hemma med familjen, utan att partnern hade möjlighet till kontakt eller kontroll.

Med digital teknik försvinner många av de möjligheterna och våldet kan utövas utan att förövaren är fysiskt närvarande. Den utsatte har i stället sin förövare i fickan, och har svårt att komma undan våldet. Digitalt våld kan dessutom ske utan att den utsatte vet att partnern har koll på var hen befinner sig eller vad hen gör. Förövaren skapar en ständig närvaro som blir ett kraftfullt psykiskt verktyg för att utöva våld. Våldet blir på så sätt rumslöst och den utsattes livsutrymme krymper.

Detta innebär inte bara förlorad frihet, utan leder ofta även till psykisk ohälsa. Att alltid vara uppkopplad och därför också ständigt sårbar, samt att aldrig kunna undkomma våldet och partnern, är extremt påfrestande för den som utsätts.

Vanliga former av digitalt våld

Precis som det i den fysiska världen finns en mängd olika sätt att skada och använda våld mot en partner, finns det även olika sätt att använda våld digitalt. För att kunna skydda barn och unga är det viktigt att du som vuxen känner till de olika sätt det digitala våldet kan ta sig i uttryck.

Digitalt psykiskt våld

Psykiskt våld som utövas digitalt är den absolut vanligaste formen av våld som unga utsätts för i parrelationer idag (Stiftelsen Allmänna Barnhuset & Jämställdhetsmyndigheten, 2024). Psykiskt våld kan se ut på en mängd olika sätt, men syftar alltid till att bryta ner den utsattes självförtroende och självkänsla.

Det kan handla om att hota, skrämma, förnedra eller kränka den utsatte. Det kan också handla om isolering, där den utsatte inte får träffa vänner, utöva fritidsaktiviteter eller röra sig fritt.

Psykiskt våld kommer ofta smygande, vilket kan göra det svårt att se eller förstå att man själv eller någon i ens närhet utsätts för det. Ofta sker detta på ett manipulativt sätt, där den utsatte personen successivt börjar internalisera den våldsamma partnerns negativa syn på sig själv.

Psykiskt våld kan utövas digitalt genom exempelvis kränkande eller hotfulla sms, upprepade samtal, krav på tillgång till lösenord, krav på aktiverade GPS-funktioner i telefonen, kontroll över vem den utsatte umgås med digitalt eller spridning av känslig information och bilder.
Psykiskt våld eller psykisk misshandel är inte ett eget brott i brottsbalken, men vissa saker, som exempelvis hot, kan vara brottsligt.

Digitalt sexuellt våld

Sexuellt våld beskrivs ofta som den typ av våld som är svårast att prata om. Många har svårt att sätta ord på sina upplevelser, vilket gör det svårt att berätta om att man blivit utsatt. Trots det vet vi att en stor del av unga har utsatts för sexuellt våld. En studie från Stiftelsen Allmänna Barnhuset och Jämställdhetsmyndigheten (2024) visar att var tionde elev i årskurs 9 har blivit utsatt för någon form av sexuellt våld av en partner.

Sexuellt våld handlar om sexuella kränkningar eller handlingar som sker utan en persons samtycke, alltså att någon gör eller säger något sexuellt mot en person utan att hen vill. Sexuellt våld handlar dock inte om sex, utan är precis som andra former av våld ett sätt att utöva makt och kontroll.

Sexuellt våld kan vara förnedring, kommentarer, trakasserier eller våldtäkt. Det kan också handla om att tvinga någon att titta på pornografi eller att ställa upp på sexuella handlingar genom hot.

Sexuellt våld kan utövas digitalt genom att skicka oönskade sexuella meddelanden eller kommentarer, ta sexuella bilder eller videor utan samtycke, tvinga någon att skicka sexuella bilder eller videor, lägga ut sexuella bilder eller videor på pornografiska hemsidor (så kallad hämndporr) eller att sprida sexuella bilder och videor. Det förekommer också att förövare filmar eller fotograferar sexuella övergrepp för att använda som utpressning eller för att sprida.

När man pratar om sexuellt våld och digital teknik är det också vanligt att nämna grooming. Grooming innebär att en vuxen tar kontakt med ett barn i ett sexuellt syfte. Fenomenet har funnits länge, men internet har gjort det möjligt för förövare att ta kontakt med barn via spel, chattar eller sociala medier. Du kan läsa mer om grooming hos Ecpat Sverige (2024).

Digitalt ekonomiskt våld

Ekonomiskt våld är vanligt förekommande idag och kan allvarligt begränsa den som utsätts. Denna typ av våld handlar också om makt och kontroll över en partner, där makten utövas genom att ta kontroll över den utsattes ekonomi. Även om ekonomiskt våld sannolikt är vanligare i vuxnas relationer, är det viktigt att unga själva och vi som vuxna förstår riskerna och konsekvenserna av ekonomiskt våld. Särskilt eftersom ungdomar redan i 13-årsåldern kan skaffa BankID och därmed använda tjänster som Swish.

Ekonomiskt våld kan handla om att kontrollera kvitton och inköp, inte tillåta den utsatte att ha egna pengar, inte tillåta den utsatte att arbeta eller att ta lån i den utsattes namn och därmed ofrivilligt skuldsätta personen.

Ekonomiskt våld kan utövas digitalt genom att ta lån i den utsattes namn via BankID eller genom hot tvinga den utsatte att föra över pengar. Det har också blivit allt vanligare att bli indragen i penningtvätt, där en förövare kan tvinga den utsatte att agera målvakt genom att ta emot och vidarebefordra pengar via exempelvis Swish.

Swish kan också göra det möjligt för förövare att kommunicera, trots att den utsatte kan ha blockerat hen överallt, genom att skicka meddelanden via appen.

Nätmobbning

Nätmobbning eller näthat är något som blivit allt vanligare hos unga i och med den ökade användningen av internet och sociala medier.

Nätmobbning handlar om att utsätta någon för kränkningar eller mobbning på nätet, i sociala medier eller i exempelvis onlinespel. Dessa kränkningar kan vara fysiska, verbala, psykiska och sexuella och är definitionsmässigt våldsamma. Du kan läsa mer om nätmobbning hos Friends (2024).

Så vanligt är våld i ungas relationer

Våld i nära relationer har länge setts som ett fenomen som bara vuxna utsätts för. Det är först under de senaste åren som omfattningen och konsekvenserna av våld i ungas parrelationer har börjat utforskas. Studier, forskning och statistik visar dock att våldet bland unga, och i synnerhet det digitala våldet, både är utbrett och startar i tidig ålder.

- **Var tredje elev i årskurs nio som dejtat/haft en relation har utsatts för någon form av våld.** *(Stiftelsen Allmänna Barnhuset & Jämställdhetsmyndigheten, 2024)*

- **Unga är i hög utsträckning både utsatta för och utövar våld i egna relationer.** *(Stiftelsen Allmänna Barnhuset & Jämställdhetsmyndigheten, 2024)*

- **60 % av ungdomar i åldern 15–19 har erfarenhet av våld i nära relationer och den vanligaste formen av våld är psykiskt våld som utövas digitalt.** *(Stiftelsen Allmänna Barnhuset & Jämställdhetsmyndigheten, 2024)*

- **84 % av föräldrar anser sig ha för lite kunskap om våld i ungas relationer.** *(Ungarelationer.se, 2024c)*

- **1 av 8 barn i åldern 12–19 år har fått nakenbilder skickade till sig. Det är särskilt vanligt bland flickor, där nästan var sjätte flicka har varit med om det.** *(Internetstiftelsen, 2023)*

- **Nästan 1 av 10 flickor i åldern 12–19 år har blivit tillfrågade om att skicka nakenbilder på sig själva mot betalning.** *(Internetstiftelsen, 2023)*

- **När unga skickar nakenbilder skickar de ofta dessa till någon de känner eller är tillsammans med. Bland gymnasieungdomar har nästan 1 av 10 skickat nakenbilder.** *(Internetstiftelsen, 2023)*

Utsatthet för våld i tidig ålder kan få långvariga effekter, både vad gäller den psykiska hälsan och svårigheter i framtida relationer. Förutom att fler insatser behöver riktas mot problemet behöver också insamlingen av statistik, data och forskning fortsätta för att bättre förstå trender och mönster (Uppsala universitet, 2024).

Exempel på digitalt våld i ungas parrelationer

Många unga berättar att de önskar att vuxna haft mer kunskap om våld i relationer. De berättar också att deras relationer ofta blir nedvärderade och inte tagna på lika stort allvar som vuxnas relationer, även när de berättar om våld.

Vill vi förebygga våld är det viktigt att inte trivialisera ungas parrelationer eller våld. Många unga vill också lära sig mer om olika typer av våld samt prata och lära sig mer om vad som är en bra eller dålig relation. Studier visar dessutom att vuxnas reaktioner på våldet ofta har stor betydelse för om det upphör eller inte. Nedan följer några exempel på hur digitalt våld, och specifikt digitalt våld i en parrelation, kan ta sig uttryck:

- **Att en partner smygläser SMS, meddelanden eller mejl**
- **Att en partner vill ta/tar reda på lösenord som bevis på kärlek eller ärlighet**
- **Att en partner bestämmer vem den andra får bli vän med, följa samt ta bort eller blocka i sociala medier**
- **Att en partner skriver och postar saker från den andras konton/mobil utan lov, eller låtsats vara någon annan**
- **Att en partner sprider privata och/eller sexuella bilder/filmer till vänner, andra eller lägger upp på porrsidor**
- **Att en partner tvingar eller i smyg laddar ner en app på den utsattes mobil som gör att den kan hålla koll på hen**

Andra exempel på digitalt våld

- **Att sprida rykten eller privat information digitalt**
- **Att skicka hot eller elaka meddelanden**
- **Att fortsätta skicka SMS/meddelanden trots att den utsatte ber partnern att sluta**
- **Att skapa falska profiler, så kallade exposekonton, för att övervaka eller trakassera någon online**

Många av dessa exempel är tätt förknippade med kontroll. Men det är inte alltid helt enkelt att skilja mellan en partner som visar omtanke genom att vara intresserad av den andras liv och en partner som övergår till ett kontrollerande beteende. Det viktigaste är att vara uppmärksam och dels prata om vilka förväntningar man har på varandra, dels prata om vad som är viktigt för en i en schysst och sund relation.

Lagar och rättigheter

En del digitala våldsgärningar kan vara straffbara enligt svensk lag. Nedan har vi listat brott som kan vara aktuella när en person utsatt någon för våld via digital teknik.

- **Ofredande**
- **Olaga förföljelse**
- **Olaga integritetsintrång**
- **Olovlig identitetsanvändning**
- **Olovlig avlyssning**
- **Dataintrång**
- **Kränkande fotografering**

Ofredande:

En person som antastar och/eller utsätter någon annan för störande kontakter eller annat hänsynslöst agerande kan dömas till ofredande. Gärningen måste vara ägnad att kränka den utsattes frid på ett kännbart sätt. Ofredande kan innefatta upprepade oönskade kontakter, till exempel telefonsamtal (Åklagarmyndigheten, 2024a).

Olaga förföljelse:

Med olaga förföljelse menas att en gärningsperson begår upprepade brottsliga handlingar mot en och samma person. Internetstalkning i Sverige betraktas som ett brott under olaga förföljelse, oavsett om det sker fysiskt eller online. Det innebär att förövaren till exempel använder internet och sociala medier för att förfölja, kontakta och övervaka den utsatte personen. Detta kan ske genom att systematiskt kommentera, gilla inlägg, skicka meddelanden, tagga eller använda fejkkonton för att nå personen, trots att denne bett om att bli lämnad ifred (Åklagarmyndigheten, 2024b).

Olaga integritetsintrång:

Olaga integritetsintrång innebär att någon gör intrång i någons privatliv genom att exempelvis sprida bilder eller information om en annan person. Bilderna och/eller informationen kan handla om någons sexualliv, hälsotillstånd eller innehålla uppgifter om att någon utsatts för ett brott som innefattar ett angrepp mot person, frihet eller frid. Det kan också vara bilder på någon som befinner sig i en mycket utsatt situation eller bilder på någons helt eller delvis nakna kropp (Brottsoffermyndigheten, 2024a).

Olovlig identitetsanvändning:

Olovlig identitetsanvändning handlar om att använda någon annans identitetsuppgifter utan tillstånd. En gärningsperson som använder en annan persons identitetsuppgifter och utger sig för att vara personen, och därmed ger upphov till skada eller olägenhet för personen, kan dömas för olovlig identitetsanvändning (Brottsoffermyndigheten, 2024b).

Olovlig avlyssning:

Det är olagligt att i smyg avlyssna någon med tekniska hjälpmedel, om personen själv inte deltar i samtalet. Det är bara tillåtet att spela in ett samtal du själv deltar i om samtalet sker mellan två personer. Är samtalet mellan fler än två personer är det olagligt att avlyssna det, även om du själv deltar i samtalet (Lagen.nu, 2024).

Dataintrång:

Ett försök att olovligen skaffa sig tillgång till någons dator eller konto på sociala medier och dess innehåll. Syftet är att få tag på privata eller hemliga uppgifter som lösenord och dokument (Polismyndigheten, 2024a).

Kränkande fotografering:

Det är olagligt att i smyg fota någon i en bostad, på en toalett, i ett omklädningsrum eller liknande utrymme. Gärningspersonen kan göra sig skyldig till kränkande fotografering. Anmälningar om kränkande fotografering rör ofta naket och/eller sexuellt innehåll som gärningspersonen sprider eller hotar att sprida (Sveriges riksdag, 2024).

Bilder samt appar och tjänster som använder sig av bilder är mycket vanliga bland unga idag. Ett fenomen som har blivit allt vanligare är att ta och dela nakenbilder med en partner. När det gäller just nakenbilder är det särskilt viktigt att vara medveten om vilka lagar som gäller, eftersom det finns situationer där delning av sådana bilder kan vara brottslig (Polismyndigheten, 2024b).

Exempel på situationer som kan vara brottsliga

Situation	Brott
Någon har skickat en nakenbild till dig utan att du har samtyckt till det	Sexuellt ofredande
Någon har skickat nakenbilder/filmer på ett barn under 18 år i en gruppchatt	Barnpornografibrott
Någon har postat nakenbilder/filmer på ett barn under 18 år på ett anonymt exposekonto	Barnpornografibrott
Någon pressar dig som är under 18 år att skicka nakenbilder. Det kan vara en partner/kompis vuxen eller någon du inte känner	Försök till utnyttjande av barn för sexuell posering
Någon hotar dig som är under 18 år med att sprida nakenbilder på dig om du inte skickar fler nakenbilder	Grovt utnyttjande av barn för sexuell posering
Någon sprider bilder, filmer eller annan känslig information om dig för att skada dig. Förutom bilder eller filmer kan det till exempel handla om uppgifter eller information om din sexualitet, din fysiska eller psykiska hälsa	Olaga integritetsintrång

Tabell skapad av Föreningen Tillsammans (2024).

Digital säkerhet

Säkerhet i den digitala världen

I takt med att allt mer av våra liv flyttar över till den digitala världen, blir frågan om säkerhet allt mer kritisk. Att känna till och hantera de risker som den ständigt föränderliga tekniken medför är därför avgörande för att skydda vår och våra barns integritet och säkerhet på nätet.

Det är viktigt att göra medvetna avvägningar när det gäller digital säkerhet – ju större risk eller utsatthet, desto fler och kraftfullare åtgärder krävs. Grundläggande kunskaper om hur man skyddar sig digitalt utgör en nödvändig bas för att bygga upp ett säkert försvar och för att kunna förstå och hantera potentiella risker.

Teknik är dock ett område i ständig förändring. Nya enheter, appar och funktioner introduceras hela tiden, medan de som finns kan förändras eller tas bort. Tänk därför på att rekommendationerna i den här foldern kan bli inaktuella, och att det är viktigt att hålla sig uppdaterad i ämnet.

Platstjänster

Platstjänster kan vara praktiska verktyg för att navigera, spåra förlorade enheter eller använda platsbaserade funktioner i sociala medier. Men dessa tjänster kan också utnyttjas i övervakande syfte, exempelvis av en våldsam partner.

Övervakning genom platstjänster

Platstjänster är funktioner på enheter som mobiltelefoner, surfplattor och datorer som använder GPS, Wi-Fi, mobilnätverk och andra tekniker för att visa var en person befinner sig. Platstjänster används exempelvis i karttjänster, platsbaserade taggar i sociala medier och säkerhetsfunktioner för att spåra förlorade enheter.

Platstjänster kan bidra till bekväma tjänster i exempelvis en telefon, men de kan också skapa säkerhetsrisker. Via mobiltelefoner kan platstjänster till exempel användas av en våldsam partner för att övervaka och kontrollera en persons rörelser i realtid via exempelvis appar eller funktioner som Snapchat, Hitta min Iphone eller Google Maps.

Fysisk tillgång till varandras digitala enheter gör det också betydligt lättare att ändra inställningar eller installera appar. När en person har fysisk åtkomst till en annan persons telefon – i kombination med kännedom om telefonens pinkod – kan den enkelt låsa upp enheten, navigera genom inställningar och installera appar utan ägarens vetskap. Detta kan bland annat innefatta att ändra säkerhetsinställningar, aktivera platsdelning och installera övervakningsprogram eller spionappar som kan ge obehörig åtkomst till meddelanden, samtalsloggar, platsdata och andra personliga uppgifter.

För att skydda sig mot sådant missbruk är det viktigt att vara medveten om hur platstjänster fungerar och vilka appar som har tillgång till platsdata. En bra tumregel är att regelbundet granska och justera sina inställningar för platstjänster på både app- och enhetsnivå och begränsa onödig delning av platsinformation. Inte minst i hotsituationer, då det är särskilt viktigt att minimera exponeringen av sin platsinformation för att öka säkerheten.

Säkerhetsåtgärder som skyddar platsinformation

Begränsa platstjänster

Använd platstjänster sparsamt och stäng av dem när de inte behövs. Vid en hotsituation kan det vara befogat att stänga av platstjänster på hela enheten.

iPhone

Android

Kontrollera appbehörigheter

Se över vilka appar som har tillgång till platsdata och begränsa det till endast nödvändiga appar.

För iPhone: Gå till **Inställningar** > **Integritet och säkerhet** > **Platstjänster**. Justera varje app till *"Aldrig"* eller *"Endast när appen används"*.

För Android: Gå till **Inställningar** > **Appar och aviseringar** > **Appbehörigheter** > **Plats**. Justera varje app till *"Tillåt endast medan appen används"* eller *"Neka"*.

Dela aldrig pinkod

Undvik obehörig åtkomst till digitala enheter genom att aldrig dela pinkod med andra.

Använd biometrisk autentisering

Om möjligt: använd biometrisk autentisering, såsom **Face ID** eller **Touch ID**.

Säkerhetsuppdatera enheter

Håll enheten uppdaterad med de senaste säkerhetsuppdateringarna för att skydda mot sårbarheter som kan utnyttjas för att spåra plats.

För att använda Googles säkerhetskontroll loggar du in på Google-kontot och navigerar till **Säkerhet** i sidomenyn.

Sociala medier

Sociala medier är en central del av många ungas liv idag, men kan samtidigt öka risken för kontroll och övervakning i deras relationer.

Föräldrakontroll i sociala medier

Sociala medier spelar en viktig roll i ungas liv för att skapa och upprätthålla sociala kontakter, möjliggöra självuttryck samt följa och utveckla sina intressen. Plattformar som Instagram, Snapchat och TikTok är särskilt populära. Men sociala medier är också en plats där unga riskerar att utsättas för olika former av digitalt våld. I en våldsam parrelation kan sociala medier användas för att övervaka och kontrollera den utsattes plats, aktiviteter och interaktioner.

Idag erbjuder flera av de stora plattformarna på sociala medier funktioner för så kallad föräldrakontroll, med syfte att ge föräldrar insyn i och kontroll över barnets aktiviteter. Dessa funktioner kan bland annat innefatta begränsad skärmtid, synlighet, sökmöjlighet och information om vilka barnet kommunicerar med.

Föräldrakontroller kan vara ett värdefullt verktyg för att skydda barnet från olämpligt innehåll och oönskade kontakter. Men dessa funktioner kan också skapa en falsk trygghet gällande barnets säkerhet. Det finns sällan en lösning som tillgodoser alla säkerhetsbehov; det handlar snarare om att flera åtgärder tillsammans kan skapa ett effektivt skydd – inte minst kunskap och kontinuerlig dialog om ämnet. Funktioner som är utformade för att övervaka barns aktiviteter kan också missbrukas av en kontrollerande partner i samma syfte. Utöver säkerhetsaspekterna finns även integritetsfrågor att fundera över, vilket du kan läsa mer om på sidan 37, som handlar om vad du som vuxen kan göra.

Expose-konton

På senare år har fenomenet expose-konton blivit en allt vanligare företeelse bland unga. Konton på sociala medier, såsom Instagram, TikTok och Snapchat, används för att sprida rykten och intima eller kränkande bilder på andra, utan deras samtycke. Dessa konton används för att hänga ut personer offentligt, ibland även med hjälp av manipulerade bilder och information. Om ditt barn utsätts av ett expose-konto är det viktigt att dokumentera händelserna, anmäla kontot hos företaget som driver plattformen, samt hos polisen.

Instagram

Instagram är en populär sociala medieapp där man delar foton och videor. Utöver foto- och videodelning har Instagram även chatt- och kommentarsfunktioner, som gör det möjligt att socialisera med andra.

En förövare kan bland annat använda Instagram för att övervaka inlägg, kommentarer och annan aktivitet, inklusive den utsattes position om den är angiven i inläggen. Förövaren kan också kräva tillgång till den utsattes konto för att kunna kontrollera vem hen interagerar med och vad hen delar eller tvinga den utsatte att avfölja eller blockera sociala kontakter, vilket kan leda till en ökad känsla av isolering.

Genom chattfunktioner kan förövaren även skicka hotfulla eller trakasserande meddelanden, eller förödmjuka den utsatte genom negativa kommentarer eller inlägg på deras bilder och videor.

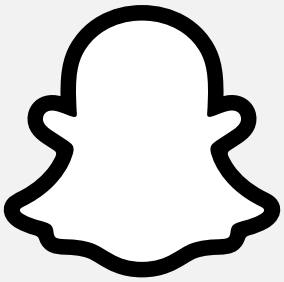
Det händer även att förövaren skapar falska profiler för att fortsätta sina trakasserier och övervakning, trots att den utsatte har blockerat förövarens vanliga konto.

Säkerhetsrekommendationer för Instagram

Använd starka lösenord: Skydda ditt konto med ett starkt, unikt lösenord och aktivera tvåfaktorsautentisering. Dela aldrig ditt lösenord med andra.

Ställ in kontot till privat: Genom att göra kontot privat kan du begränsa vem som kan se dina inlägg och kontakta dig.

Begränsa din information: Undvik att dela personlig information och var försiktig med vad du postar. Var medveten om platstaggar och undvik att dela din aktuella plats.



Snapchat

En populär app bland unga är sociala medieplattformen Snapchat. Appen låter användare skicka tidsbestämda bilder, videor och meddelanden – så kallade "snaps" – till vänner och följare, som sedan försvinner. Snapchat har även stöd för att skapa grupper, vilket är vanligt i kompisgäng och skolklasser.

En funktion som skiljer Snapchat från andra sociala medier är den så kallade "Snapkartan", som genom platstjänster och GPS gör det möjligt att se och följa var ens vänner befinner sig. Just Snapkartan är ett återkommande ämne bland unga, och något många vittnar om kan leda till ökad kontroll och övervakning. Att alltid ha på Snapkartan är för många ett måste, i synnerhet bland unga som lever i en kärleksrelation där den kan ses som ett tecken för tillit.

Andra sätt som Snapchat kan användas i ett kontrollerande syfte är att kräva eller be om regelbundna bilder som bevis för var personen befinner sig. Och trots att bilder och videor som skickas på Snapchat är tidsbestämda kan snaps som skickas i förtroende skärmdumpas och spridas utan barnets medgivande. En förövare kan även hota att sprida pinsamma eller privata bilder om ditt barn inte gör som de säger, vilket kan leda till stor ångest och rädsla.

Säkerhetsrekommendationer för Snapchat

Använd starka lösenord: Skydda ditt konto med ett starkt, unikt lösenord och aktivera tvåfaktorsautentisering. Dela aldrig ditt lösenord med andra.

Begränsa platstjänster: Aktivera "Spökläge" i "Snapkartan" för att dölja din plats för andra användare.

Tänk på vad du delar: Tänk på vilken information du delar, och var medveten om att även om snaps försvinner efter att de har visats, kan mottagaren ta skärmdumpar eller använda en annan enhet för att fota innehållet.

TikTok

TikTok är en social medieplattform där användare kan skapa, dela och titta på videor, samt kommunicera via chattfunktioner och kommentarsfält. Appen har på relativt kort tid blivit omåttligt populär – inte minst bland unga.

Men TikTok är även en plats där unga personer riskerar att utsättas för kontroll, hot och trakasserier. Precis som med andra sociala medier kan en partner använda plattformen för att kontrollera och begränsa en användare genom att övervaka dess aktivitet. Via kommentarsfält och chattfunktioner kan förövaren skicka hotfulla eller trakasserande meddelanden, eller själv skapa och sprida kränkande innehåll på den utsatte. TikToks direktmeddelandefunktion är endast tillgänglig för användare som är 16 år eller äldre. Det är dock inte en garanti för att yngre personer inte använder den, då TikTok inte verifierar användarens ålder.

Säkerhetsrekommendationer för TikTok

Använd starka lösenord: Skydda ditt konto med ett starkt, unikt lösenord och aktivera tvåfaktorsautentisering. Dela aldrig ditt lösenord med andra.

Ställ in kontot till privat: Genom att göra kontot privat kan du begränsa vem som kan se dina inlägg och kontakta dig.

Skapa en nyckel: För att förbättra säkerheten och förenkla inloggningen på TikTok, konfigurera en kryptografisk nyckel på din mobila enhet. Nyckeln lagras på enheten och använder säkerhetsfunktioner som Face ID, lösenkod och pinkod, vilket tar bort behovet av ett lösenord. Du kan även logga in från enheter anslutna till ditt Apple ID eller Google-konto.

Gå in på din profil, tryck på **Meny**-knappen och vidare till **Inställningar och sekretess**. Tryck på **Konto**, sedan **Nyckel** och därefter **Konfigurera** på nästa skärm. Följ anvisningarna som anges.

Säkerhetsrekommendationer vid oönskad kommunikation via Instagram, Snapchat och TikTok

Blockera konton

För att skydda dig mot oönskad kommunikation, börja med att blockera användarens konto. På Instagram, TikTok och Snapchat gör du detta genom att gå till personens profil, klicka på de tre prickarna i det övre högra hörnet och välja Blockera. Bekräfta sedan ditt val. Fortsätt att blockera alla nya konton som personen skapar för att kontakta dig.

Rapportera konton

Rapportera de nya kontona till respektive plattform för trakasserier eller olämpligt beteende. På Instagram och TikTok kan du göra detta från personens profil genom att klicka på de tre prickarna och välja Rapportera. På Snapchat kan du rapportera konton genom att hålla ned användarnamnet, klicka på Mer och sedan Rapportera.

Ställ in din profil till privat

Begränsa vem som kan se och kontakta dig genom att ställa in din profil till privat. På Instagram och TikTok gör du detta genom att gå till dina inställningar, välja Sekretess och aktivera Privat konto. På Snapchat kan du se till att endast dina vänner kan kontakta dig och se din story genom att justera dina sekretessinställningar.

Begränsa kommentarer och meddelanden

På TikTok och Instagram kan du begränsa vem som kan kommentera och skicka meddelanden till dig under sekretessinställningarna. Välj att endast tillåta kommentarer och meddelanden från personer du följer. Snapchat tillåter dig att begränsa vem som kan kontakta dig och hitta dig via telefonnummer eller användarnamn.

Använd ytterligare säkerhetsfunktioner

- **Filtrering av kommentarer:** På TikTok och Instagram kan du aktivera kommentarsfiltrering för att automatiskt dölja vissa ord eller fraser.

- **Begränsa på Instagram:** Instagram erbjuder en funktion som kallas "Begränsa", där kommentarer och meddelanden från begränsade personer döljs för andra.

- **Skuggblockering på Snapchat:** I stället för att bara blockera kan du ta bort personen från din vänlista och undvika att interagera med nya konton som liknar deras.

i åldern 12–19 år har fått nakenbilder skickade till sig. Det är särskilt vanligt bland flickor, där nästan var sjätte flicka har varit med om det.

(Internetstiftelsen, 2023)

Samla bevis

Ta skärmdumpar av meddelanden, kommentarer och kontakter som bevis. Detta kan vara användbart om du behöver rapportera till myndigheterna eller respektive plattform. På Snapchat, använd en annan telefon för att fotografera bilder och konversationer för att undvika att avsändaren notifieras om en skärmdump tas.

Anmäl till polisen

Om trakasserierna fortsätter och du känner dig hotad eller trakasserad, överväg att anmäla situationen till polisen. Kontinuerliga trakasserier från olika konton kan betraktas som stalkning och kan vara olagligt.

BankID och Swish

Trots att BankID och Swish är framtagna för att underlätta säkra och snabba inloggningar och betalningar, finns det en risk att dessa tjänster utnyttjas som verktyg för digitalt och ekonomiskt våld.

BankID och Swish har på kort tid blivit viktiga verktyg för svenskar i alla åldrar. BankID fungerar som en elektronisk identitet, som gör det möjligt att säkert logga in på bankkonton, myndighets-sidor och andra tjänster online.

Samtidigt har Swish revolutionerat hur vi skickar och tar emot pengar i realtid via mobilnummer, vilket gör betalningar smidigare än någonsin. Men trots att både BankID och Swish kan anses som säkra ur ett rent tekniskt perspektiv, kan dessa teknologier användas som verktyg för att utföra både digitalt och ekonomiskt våld.

BankID

En förövare som har tillgång till den enhet den utsattes BankID är kopplat till, och samtidigt känner till säkerhetskoden, kan använda kontot för att orsaka betydande skada. Förutom att få tillgång till känslig information via myndighetssidor och andra plattformar, kan förövaren genomföra transaktioner och till och med ta lån eller krediter i den utsattes namn – så kallat ekonomiskt våld. Om BankID används för att logga in på tjänster kopplade till e-post eller sociala medier, kan förövaren också övervaka den utsattes kommunikation och sociala aktiviteter.

En ytterligare risk som är viktig att vara medveten om är möjligheten att utfärda ett nytt BankID i någon annans namn. Detta kan göras via internetbanken och kräver styrkande med giltig legitimation, såsom pass eller nationellt ID-kort – något som en person man umgås med ofta kan ha tillgång till. Om en förövare skapar ett BankID och kopplar det till sin egen enhet, och samtidigt känner till offrets lösenkod, kan denne använda BankID:t obehindrat.

Säkerhetsrekommendationer för BankID

Dela inte säkerhetskoder

Lämna aldrig ifrån dig koden eller lösenordet till ditt BankID, inte ens till familjemedlemmar. Logga heller aldrig in på någon annans uppmaning. Utöver riskerna det medför strider det även mot ditt och bankens avtal, och kan leda till juridiska följder.

Håll uppsyn över misstänkt aktivitet

Kontrollera regelbundet dina bankkonton och BankID-transaktioner. Aktivera notifikationer för transaktioner och inloggningar för att snabbt upptäcka misstänkt aktivitet.

Agera vid obehörig åtkomst

Om en obehörig får kontroll över ditt BankID eller utfärdar nya BankID:n i ditt namn – spärra dessa omedelbart via internetbankens tjänst, där samtliga utfärdade BankID för ens personnummer listas och kan spärras. Byt lösenord/lösenkod på de BankID:n du använder.

Swish

Förutom risker som överkonsumtion och bedrägerier kan Swish även utgöra en fara för personer som utsätts för våld i nära relationer. Ett exempel är att bli indragen i penningtvätt, där en förövare kan tvinga den utsatte att agera målvakt genom att ta emot och vidarebefordra pengar via Swish. Ett annat är att förövaren kräver att den utsatte swishar pengar under hot om våld eller andra konsekvenser.

Möjligheten att skicka meddelanden i samband med transaktioner kan också leda till oönskad kommunikation. En förövare kan använda Swish som en alternativ kontaktväg när den har blivit blockerad på andra kommunikationsplattformar. Genom att swisha små summor pengar kan förövaren använda tjänsten för att skicka hotfulla och trakasserande meddelanden.

Säkerhetsrekommendationer för Swish

Sätt upp begränsningar

Sätt upp gränser för hur mycket pengar som kan swishas för att förhindra att stora summor pengar kan skickas och tas emot. Många banker låter dig justera Swish-inställningar via deras internetbank eller mobilapp. Logga in på din internetbank eller bankapp och leta efter Swish-inställningar.
Där kan du ofta sätta eller ändra gränser för betalningar.

Blockera användare

Vid behov går det att blockera telefonnummer från att swisha. Det är dock endast möjligt om telefonnumret redan har skickat en överföring vid ett tidigare tillfälle. Gå till fliken **Historik** och klicka på den aktuella transaktionen. Klicka sedan på **Visa betalningshistorik**, därefter på de tre prickarna i högra hörnet och sedan på **Blockera avsändare**.

Molntjänster

Molntjänster, såsom iCloud och Google Cloud, underlättar lagring och åtkomst till data. Men dessa tjänster kan också bli effektiva verktyg för den som vill övervaka en partners digitala aktiviteter.

Molntjänster

Molntjänster lagrar data på fjärrservrar som hanteras av tjänsteleverantörer som Google, Apple eller Microsoft. Med hjälp av molntjänster kan man ladda upp, spara och komma åt data, såsom foton, videor, dokument, e-post, kontakter och kalendrar, via internet från vilken enhet som helst.

Molntjänster kan dock innebära risker för personer som utsätts för våld i nära relation. Om en förövare får tillgång till den utsattes molnkonto som är kopplad till en mobil enhet, exempelvis iCloud, kan den övervaka all aktivitet, inklusive få tillgång till känslig information, spåra rörelser genom platsdata, ändra kontoinställningar och ta bort eller ändra innehåll. Detta kan ske om den utsatte har loggat in på sitt molnkonto på förövarens enhet eller om förövaren har kännedom om lösenordet. Det är med andra ord oerhört viktigt att aldrig dela med sig av sitt lösenord till sina mobila molnkonton.

Funktioner som använder molntjänster, såsom familjedelning och Find My iPhone/Find My Device, kan också missbrukas av en förövare för att övervaka den utsattes position i realtid.

Säkerhetsrekommendationer för molntjänster

Lösenordssäkerhet

Använd starka, unika lösenord på samtliga molntjänster. Vid behov: ändra lösenordet för din molntjänst för att säkerställa att endast du har tillgång.

Aktivera tvåfaktorsautentisering

Aktivera tvåfaktorsautentisering för att lägga till ett extra säkerhetslager. Detta kräver att alla enheter som försöker logga in på ditt konto måste verifiera sig med en extra kod.

Granska behöriga enheter

Kontrollera att inga obehöriga enheter är anslutna till dina molntjänster.

För Android: Gå till **Google-konto** > **Säkerhet** > Dina enheter och kontrollera om det finns okända enheter. Gå även till **Inställningar** > **Säkerhet** > Hitta min enhet för att se om någon annan enhet är registrerad.

För iOS: Gå till **Inställningar** > **[Ditt namn]** och se om det finns okända enheter listade under ditt Apple ID. Gå även till **Inställningar** > **[Ditt namn]** > **Hitta** > **Hitta min iPhone** och kontrollera listan över enheter.

Granska appbehörigheter

Kontrollera vilka appar som har åtkomst till din molntjänst och återkalla åtkomst för de som inte är nödvändiga.

Granska vilken information som lagras

Se över vilken information som lagras i respektive tjänst. Det går exempelvis att välja om sökhistorik och platsinformation ska lagras via Google-kontot, eller om iCloud ska lagra meddelanden, e-post och bilder.

Övervaka inloggningsaktiviteter

Håll ett öga på inloggningsaktiviteter och få notifikationer vid nya inloggningar eller misstänkt aktivitet.

Logga ut från alla enheter

Många molntjänster erbjuder alternativet att logga ut från alla enheter. Detta säkerställer att alla sessioner avslutas och kräver en ny inloggning.

Viktigt!

Om du byter telefon och misstänker att någon har tillgång till dina nuvarande molnkonton, är det viktigt att skapa nya molnkonton i samband med att du skaffar den nya enheten. Annars riskerar du att den som har tillgång till dina gamla konton kan få kontroll över din nya telefon när du loggar in med de gamla inloggningsuppgifterna.

Lösenord och säkra konton

Starka och unika lösenord är en av de viktigaste åtgärderna man kan vidta för att öka sin digitala säkerhet.

Många använder lösenord som är enkla att komma ihåg, baserade på ord och siffror som bär mening för användaren. Det kan handla om födelsedatum, adress eller namn på husdjur och familjemedlemmar. Lösenord som består av dessa komponenter är inte sällan enkla för någon som haft en nära relation med användaren att gissa sig till.

Idag ställer de flesta tjänster krav på att lösenord som skapas ska vara av en viss längd och innehålla små och stora bokstäver, siffror och specialtecken. Att använda långa lösenord är bra, men att inte återanvända lösenord till olika tjänster är viktigare, då lösenord som förekommer i lösenordsläckor från en tjänst kan användas för att komma åt andra konton.

Ett konto som är extra viktigt att skydda med ett starkt lösenord är e-postadressen, som ofta fungerar som en knutpunkt för alla konton på nätet. E-postadressen är knuten till ett stort antal sociala medier, betaltjänster, medlemssidor, molntjänster och ID-tjänster för telefon eller dator. Om någon har lösenordet till en annan e-postadress kan den få tillgång till de konton som är kopplade till e-postadressen genom en enkel lösenordsåterställning, och på så sätt ta över, övervaka eller stänga ute personen från sina konton.

Kännetecken för ett säkert lösenord:

- **Är unikt**
- **Innehåller inte ord eller namn som återfinns i ordlistor**
- **Innehåller inte ord eller siffror som är lätta att gissa sig till, eller som innehåller personliga referenser**
- **Delas inte med någon annan**
- **Har en säker återställningsmetod**

Verktyg för ökad lösenordssäkerhet

Tvåfaktorsautentisering

Tvåfaktorsautentisering – ibland kallat tvåstegsautentisering eller multifaktorsautentisering – innebär ett extra steg, utöver lösenordet, för att visa att du verkligen är du. Vanligtvis sker tvåfaktorsautentisering genom att en verifikationskod skickas som ett sms eller e-post till dig efter att du angett ditt lösenord, alternativt via en genererad kod i en app. Använd tvåfaktorsautentisering till alla tjänster där det är möjligt. Särskilt viktigt är det att använda tvåfaktorsautentisering för betaltjänster, e-post, sociala medier och lagringstjänster.

Lösenordshanterare

En lösenordshanterare är ett program som ger förslag på långa, säkra och unika lösenord, sparar lösenorden i ett krypterat valv och hjälper dig att komma ihåg lösenorden när de ska användas. En lösenordshanterare gör det möjligt att ha komplexa, säkra lösenord, utan att du behöver oroa dig för att glömma bort dem.

Observera att en lösenordshanterare kan vara en dålig idé om förövaren har tillgång till enheten.

Inbyggda säkerhetsfunktioner i iPhone och Google

iPhones säkerhetskontroll

Säkerhetskontroll är en funktion i iPhone som är utformad för att hjälpa användare att hantera och skydda sina personliga data och integritet, särskilt i situationer där de kan vara utsatta för digitalt våld eller trakasserier. Denna funktion gör det möjligt att snabbt återställa och granska delningar av platsdata, appåtkomst och andra inställningar. Funktionen kräver att telefonen är uppdaterad till iOS 16 eller senare, och att det finns ett Apple-ID med tvåfaktorsautentisering.

För att använda iPhones säkerhetskontroll går du till **Inställningar** i telefonen, därefter vidare till **Integritet och säkerhet** och väljer sedan **Säkerhetskontroll**.

Googles säkerhetskontroll

Googles Säkerhetskontroll (Security Checkup) förbättrar säkerheten för Google-konton genom att ge en översikt över kontosäkerheten. Där går det bland annat att kontrollera inloggningar och enheter för att logga ut från obekanta enheter, granska säkerhetsaktiviteter, hantera åtkomst för tredjepartsappar, aktivera tvåfaktorsautentisering och justera återställningsinformation (som telefonnummer och e-postadresser) för att säkerställa enkel kontoåterställning.

För att använda Googles säkerhetskontroll loggar du in på ditt Google-konto och navigerar till **Säkerhet** i sidomenyn.


Vad kan jag som vuxen göra?

Hur du pratar med ditt barn om digitalt våld

Att förstå och följa med i ungas digitala värld kan vara utmanande för vuxna, samtidigt som det spelar en avgörande roll för att skydda dem från digitalt våld och främja hälsosamma relationer. Genom att ha öppna samtal om kärlek, kontroll och integritet på nätet kan du som vuxen hjälpa ditt barn att reflektera över sitt beteende online och upptäcka potentiella risker.

Det kan vara utmanande att som vuxna navigera i både ungas sociala liv och i den digitala världen. Särskilt svårt kan det kännas att förstå och hantera de olika plattformarna som barn och unga använder och hur dessa plattformar är sammanbundna med ungas socialisering och relationer.

För att på bästa sätt skydda unga från digitalt våld är det viktigt att sätta sig in i och utbilda sig om vilka plattformar unga använder, hur de fungerar och hur de påverkar deras liv. Genom att göra detta blir det lättare att identifiera och förstå de risker som kan vara förknippade med dessa plattformar.

Prata om kärlek och kontroll

Eftersom linjen mellan en partner som visar kärlek, tillit och omtanke och en partner som kontrollerar och isolerar kan vara svår för unga att identifiera behöver de stöd i att navigera sina relationer från oss vuxna.

Som vuxen kan du prata med ditt barn om vad som är ett hälsosamt sätt att interagera med en partner på med hjälp av digital teknik. Samtala med ditt barn om förväntningar i en relation och riskerna med att känna att man måste leva upp till dessa, även när man inte mår bra av det. Försök stötta ditt barn i att själv identifiera vilka förväntningar hen känner sig bekväm med. Det kan du göra genom att ställa frågor för att stötta hen i att reflektera över kärlek, kontroll och linjen där emellan.

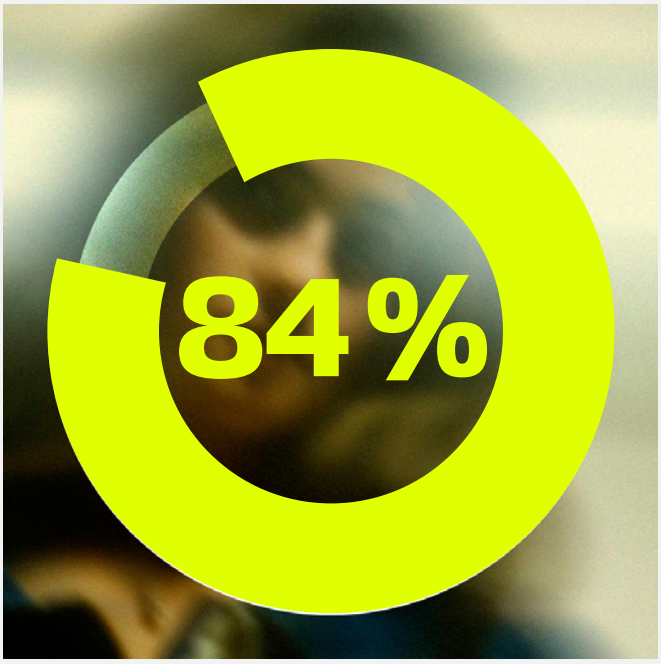
Fråga: Hur tänker du att man kan visa kärlek mot en partner digitalt?

Fråga: Vad tycker du att en partner ska ha tillgång till på din telefon?

Fråga: Måste man dela sin pinkod med sin partner? Varför/Varför inte?

Fråga: Måste man ha Snapkartan aktiverad för sin partner? Varför/Varför inte?

Här kan det vara viktigt att samtala utan att vara alarmistisk. Om vi bara pratar om risker eller faror är det vanligt att unga slutar lyssna. I stället är det bättre att fokusera på en öppen dialog där de kan prata om sina tankar, reflektioner och upplevelser.



av föräldrar anser sig ha för lite kunskap om våld i ungas relationer.

(Ungarelationer.se, 2024c)

Prata om hur man behandlar andra

Barn och unga saknar ofta ett fullständigt utvecklat konsekvenstänk. De kan ha svårt att förstå komplexa samband och hur deras handlingar påverkar både dem själva och andra. Här kan du som vuxen hjälpa dem att förstå genom att diskutera konkreta exempel och hur goda intentioner kan leda till negativa konsekvenser.

Fråga: Vilka typer av meddelanden tycker du är okej att skicka till en partner?

Fråga: Vilken typ av bilder på någon annan är okej att dela med andra?

Fråga: Hur känner du om din partner inte svarar på dina meddelanden direkt?

För många unga har det blivit en integrerad del av vardagen att dela med sig av sitt liv via bilder, videor, meddelanden eller platstjänster, vilket kan göra det svårt att avgöra vad som är okej eller inte.

Det är viktigt att påminna om att hur de agerar online bör reflektera hur de själva vill bli behandlade. Det kan också vara viktigt att prata om att krav på tillgänglighet från en partner, via exem-

pelvis platstjänster, bilder eller meddelanden, även med goda avsikter, kan kränka partnerns integritet eller få hen att må dåligt.

Prata för att skapa trygghet

Studier och forskning visar att unga sällan pratar med vuxna om de utsätts för våld, hot och kränkningar (Korkmaz & Överlien, 2023). För att på bästa sätt stötta och skydda ditt barn från digitalt våld är det därför viktigt att du försöker bygga en stark och tillitsfull relation. Här blir arbetet hemma i vardagen nyckeln.

Ha regelbundna samtal om respekt, kärlek och ansvar online och försök skapa en miljö där ditt barn känner sig trygg med att dela med sig. Uppmuntra till att dela med sig och var närvarande och engagerad. Genom att regelbundet prata om dessa frågor, både högt och lågt, bygger du en trygg grund där ditt barn känner sig hörd och förstådd.

Prata om relaterbara situationer

När en händelse kopplad till relationer, sociala medier eller internet sker, exempelvis för en influencer, kändis eller kanske någon i ditt barns umgänge, kan det vara en bra ingång till samtal. Diskutera situationen för att hjälpa dem att reflektera över vad som är ett lämpligt beteende online.

Fråga: Vad tänker du om hur den här personen betedde sig?

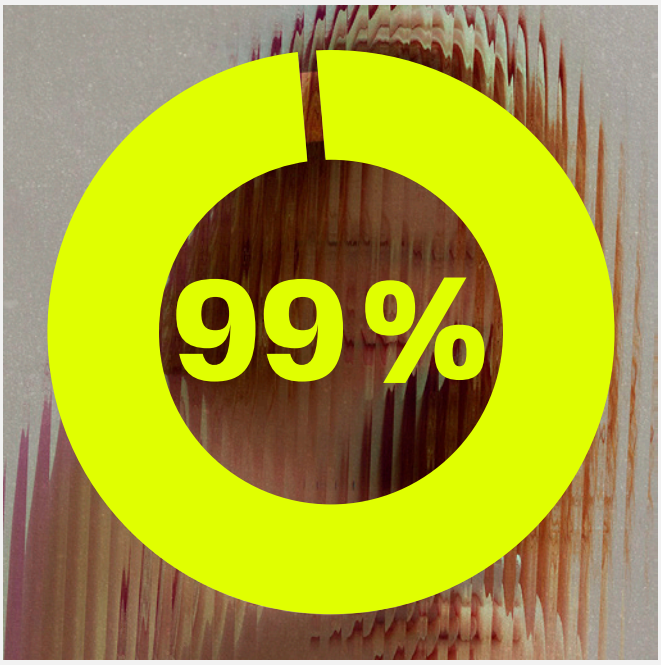
Fråga: Vad tänker du hade varit ett bättre sätt att hantera situationen på?

Så gör du om något har hänt

Om något händer eller har hänt online, är det viktigt att reagera på ett genomtänkt och lugnt sätt. Visa att du tar situationen på allvar, även om den kan verka banal vid en första anblick. Många unga berättar att vuxna förminskar deras upplevelser av våld, att de inte tas på allvar just för att de är unga. Dessutom saknar unga ofta själva referensramar för vad som är allvarligt – vifta därför inte bort deras oro eller upplevelser. Samla information och ställ frågor i stället för att direkt ge råd. Detta skapar en dialog och hjälper dig att förstå situationen bättre.

Vid allvarliga händelser är det viktigt att samla bevis. Använd en annan telefon för att ta bilder av skärmen om det behövs, eftersom vissa appar informerar användaren om skärmdumpar tas. Kom ihåg att det inte är din uppgift att avgöra om något är ett brott. Om ditt barn utsatts för något obehagligt – agera och gör en polisanmälan! Genom att göra en polisanmälan bidrar du även till insamlandet av viktig statistik som kan leda till öka medvetenheten om brott på nätet.

För att ditt barn ska känna sig trygg att berätta om sina upplevelser online, är som sagt tillitsfulla relationer avgörande. Prata regelbundet med ditt barn och andra föräldrar. Om ditt barn berättar om en incident på nätet, lova inte något du inte kan hålla, men försäkra dem om att du kommer göra ditt yttersta för att hjälpa. Förklara att din initiala reaktion kan vara känslomässig, men att du kommer att lugna ner dig och agera rationellt (Prinsparets stiftelse, 2024).



av barn och unga i åldern 8–19 år använder internet.

Svenskarna och internet (2023)

Gör det tydligt för barnet att du tror på det. Det finns rädsla i att inte bli trodd på grund av påförande av skuld och skam. Ge barnet tid och utrymme samt lyssna. Bekräfta deras mod att anförtro sig till dig genom att ge dem full uppmärksamhet. Sök ögonkontakt, ha ett öppet kroppsspråk och försök att inte byta samtalsämne. Låt dem ta sin tid att berätta för dig.

Slutligen är det viktigt att ge ditt barn verktyg om det stöter på olämpligt innehåll på nätet, exempelvis om det ser olagliga bilder eller videor. Berätta att man inte ska sprida vidare materialet utan i stället visa för en vuxen som man litar på och/eller eventuellt göra polisanmälan.

Föräldrakontroll och dubbla signaler

Som vuxna har vi ett ansvar och känner ofta ett stort behov av att skydda våra barn. Digital teknik har på många sätt gjort det möjligt för vuxna att ha bättre koll på barn och unga och deras rörelsemönster, samt vilka de umgås och socialiserar med.

Idag är det vanligt att föräldrar ber sina barn att skicka sms för att berätta var de befinner sig, vem de är med och när de kommer hem. Det är heller inte ovanligt att använda appar med platstjänster eller GPS-klockor för att hålla koll på var barnet befinner sig.

Det finns ingen åldersgräns för när föräldrar och vuxna får eller inte får titta i sitt barns telefon, eller kontrollera var barnet befinner sig. I Sverige finns inte den typen av rättsliga regler alls. Däremot har barn och unga rätt till ett privatliv och rätt till integritet, och faktiskt också rätt att ha lite hemligheter från föräldrar (Barnombudsmannen, 2024).

Å andra sidan har vårdnadshavare ett ansvar att se till att barn och unga inte kommer till skada och inte heller skadar andra. Dessutom kan barn och unga under 13 år inte samtycka till att deras personuppgifter behandlas och kan därför egentligen inte ha konton på sociala medier självständigt (Integritetsmyndigheten, 2024).

Det betyder att barn och unga bör vara under vuxnas uppsikt när de använder sociala medier. Ofta är det just detta ansvar samt omtanke som föräldrar och vuxna refererar till när de har överenskommelser med barnet om att skicka sms, kontrollera var barnet befinner sig eller få insyn i barnets aktivitet på sociala medier.

När föräldrakontroll används av vuxna, samt motiveras och förklaras som ett uttryck av omtanke och kärlek, är det viktigt att fundera kring vilka signaler det skickar ut om kärlek och kontroll i en nära relation. I sammanhanget blir det oerhört viktigt att förklara att det är skillnad på olika relationer.

Om du som vuxen använder olika former av föräldrakontroll (exempelvis via en eller flera appar), bör du prata med barnet om varför du gör det. Framför allt kan det vara bra att prata om att det i en kärleksrelation inte är ett tecken på omtanke eller kärlek att hålla koll på var en partner befinner sig, vem partnern umgås med eller kräva att ha platstjänster på (Ungarelationer.se, 2024).

Varningssignaler vid våld

Alla reagerar olika när de blir utsatta för våld, och det finns inget rätt eller "normalt" sätt att känna eller agera på. Det är därför viktigt att du som vuxen är uppmärksam på förändringar i ditt barns beteende, då det kan vara en signal på att något är fel.

Även om det inte finns något rätt eller normalt sätt att reagera på, finns det olika varningssignaler på att ditt barn utsätts för våld, som du kan hålla utkik efter.

- **Vill sällan göra saker utan sin partner**
- **Måste alltid svara direkt på meddelanden eller samtal från partnern**
- **Partnern ringer eller skriver överdrivet mycket**
- **Partnern vill hela tiden veta var hen är eller vem hen är med**
- **Drar sig undan från vänner och familj**
- **Slutar med fritidsintressen eller aktiviteter**
- **Har bristande intresse för saker hen tidigare uppskattade**
- **Får minskad självkänsla och tvivlar mer på sig själv**
- **Visar ökad irritabilitet, ilska eller frustration, särskilt i samband med användning av telefon eller sociala medier**
- **Upplever nedstämdhet och ångest**

Mer allvarliga händelser eller långvarig utsatthet för våld kan leda till depression, vilket kan yttra sig i känslor av hopplöshet och sorg. Ditt barn kan då dra sig undan helt från exempelvis sociala medier och telefonen eller bli överdrivet upptagen med dem (1177.se, 2024).

Om du märker att ditt barns personlighet förändras – ta det på allvar och försök ta reda på vad som kan ligga bakom. Prata med skolan och andra föräldrar för att få en helhetsbild.

Resurser och stöd

Här har vi listat några av de verksamheter och organisationer som både utsatta och närstående kan vända sig till för att få tips, råd och hjälp. Som förälder får du också gärna tipsa barn och unga du känner om vår hemsida digitalctrl.se.

Digitala lektioner (Internetstiftelsen)

Plattform som erbjuder kostnadsfria, kvalitetssäkrade lektionsmaterial för att stärka elevers digitala kompetens och förståelse för internetanvändning i skolan.

ECPAT

Ideell organisation som arbetar för att förebygga och bekämpa alla former av sexuella övergrepp mot barn, både online och offline.

Fatta

Ideell rörelse som arbetar för att stoppa sexuellt våld och främja samtycke genom opinionsbildning, utbildning och kultur.

Friends

Ideell organisation som arbetar för att förebygga mobbning och främja trygghet och respekt bland barn och unga i skolor och andra miljöer.

Föreningen Tillsammans

Ideell förening som jobbar för ett samhälle fritt från sexuellt våld och som bland annat erbjuder stödsamtal med kurator och/eller stödgrupper.

Killar.se

Samlingsplats för killar och unga män 10–25 år för att få och ge stöd. Erbjuder bland annat stödchatt söndag–torsdag klockan 19:00–21:00.

Kvinnofridslinjen

Stöd för den som utsatts för hot och våld. Öppet dygnet runt, samtalet är gratis och man kan vara anonym. Tel: 020-50 50 50

Kvinnojour/Tjejjour i din kommun

Mottagningen för unga män (MUM Online)

Sex- och relationsmottagning för den som identifierar sig som man och är mellan 18 och 30 år gammal.

Nationellt centrum för kvinnofrid (NCK)

Kunskaps- och resurscentrum vid Uppsala universitet som arbetar för att förebygga och bekämpa våld mot kvinnor genom forskning, utbildning och stödverksamhet.

Näthatshjälpen

Digital tjänst som erbjuder stöd och hjälp till unga som utsätts för nätmobbning, näthat eller andra kränkningar på internet.

Polisen

PrenvenTell

Hjälplinje vid oönskad sexualitet
Tel: 020 66 77 88

Räddabarnen.se - Kärleken är fri

Rädda Barnens satsning mot hedersrelaterat våld och förtryck med stödchatt som är öppen söndag–torsdag klockan 19:00–21:00.

Skolhälsovården/elevhälsan

Stödlinje för våldsutsatta män

Tel: 020 80 80 80

Stödlinje för våldsutsatta transpersoner

Tel: 020 55 00 00

Ungasjourer.se

Samlingsplats för alla jourer i Sverige som arbetar med att stötta och stärka barn, unga och unga vuxna.

Unga relationer.se

Nationell stöd- och kunskapsplattform för att motverka våld i ungas partnerrelationer med bland annat stödchatt varje kväll klockan 20:00–22:00.

Ungdomsmottagningen i din kommun

Unizonjourer.se

Samlingsplats för Sveriges kvinnojourer.

UMO

Ungdomsmottagning på nätet som erbjuder information, stöd och rådgivning kring hälsa, relationer och sexualitet för unga mellan 13 och 25 år.

Referenser

Rapporter

Brottsförebyggande rådet. (2021). *Våld i ungas parrelationer*. Hämtad från: https://bra.se/publikationer/arkiv/publikationer/2021-10-29-vald-i-ungas-parrelationer.html

Folkhälsomyndigheten. (2024). *Digitala medier och barns och ungas hälsa – en kunskapssammanställning*. Hämtad från: https://www.folkhalsomyndigheten.se/contentassets/20a0ad3202d54bc9be156ff3e407b55c/digitala-medier-barns-ungas-halsa-kunskapssammanstallning.pdf

Korkmaz, S., & Överlien, C. (2023). *Våld i ungas nära relationer; det ideella stödet: Möjligheter och begränsningar*. Hämtad från: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-216780

Internetstiftelsen. (2023). *Svenskarna och internet 2023*. Hämtad från: https://svenskarnaochinternet.se/app/uploads/2023/10/internetstiftelsen-svenskarna-och-internet-2023.pdf

Stiftelsen Allmänna Barnhuset, Jämställdhetsmyndigheten. (2024). *Våld i ungas nära relationer och hedersrelaterat våld och förtryck*. Hämtad från: https://allmannabarnhuset.se/product/vald-i-ungas-nara-relationer-och-hedersrelaterat-vald-och-fortryck-2/#product-info

Artiklar

Henry, N., & Powell, A. (2018). *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research*. Trauma, Violence, & Abuse, 19(2), 195–208. https://doi.org/10.1177/1524838016650189

Korkmaz, S., Överlien, C., & Lagerlöf, H. (2022). *Youth intimate partner violence: Prevalence, characteristics, associated factors and arenas of violence*. Nordic Social Work Research, 12(4), 536–551.

Øverlien, C. (2018). *Våld mellan ungdomar i nära relationer: digitala medier och utövande av kontroll*. Socialvetenskaplig Tidskrift, 25(1), 67–85. https://doi.org/10.3384/SVT.2018.25.1.2382

Webbplatser

Apple. (2024). *iPhone Användarhandbok*.
https://support.apple.com/sv-se/guide/iphone/welcome/ios

Barnombudsmannen. (1 augusti 2024). *Barnkonventionen*.
https://www.barnombudsmannen.se/barnkonventionen/

Brottsförebyggande rådet. (3 juni 2024b). *Näthat*.
https://bra.se/forebygga-brott/forebyggande-utifran-amne/nathat.html

Brottsoffermyndigheten. (3 juni 2024a). *Olaga integritetskontroll*.
https://www.brottsoffermyndigheten.se/referatsamling/referat-till-och-med-den-30-juni-2022/frihets-och-fridsbrott/olaga-integritetsintrang/

Brottsoffermyndigheten. (3 juni 2024b). *Olovlig identitetsanvändning*.
https://referatsamling.brottsoffermyndigheten.se/referat-till-och-med-den-30-juni-2022/frihets-och-fridsbrott/olovlig-identitetsanvandning/

Domstolsverket - Sveriges domstolar (4 juli 2024). *Påföljder för unga*.
https://www.domstol.se/amnen/brott-och-straff/straff-och-pafoljder/pafoljder-for-unga/

Facebook. (2024). Instagram hjälpcenter.
https://sv-se.facebook.com/help/instagram

Föreningen Tillsammans. (10 juli 2024). *Att skicka, dela vidare och ta nakenbilder*.
https://www.foreningentillsammans.se/aktuellt/om-nakenbilder-nudes

Google. (2024). *Androids säkerhets- och integritetsinställningar*.
https://support.google.com/android/answer/13985942?hl=sv

Integritetsskyddsmyndigheten. (4 juli 2024). *Det här gäller enligt GDPR*.
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/

Lagen.nu - Datorföreningen Lysator vid Linköpings universitet. (3 juni 2024). *Olovlig avlyssning*
https://lagen.nu/begrepp/Olovlig_avlyssning

Näthatshjälpen. (4 juni 2024). *Svensk lag på internet*.
https://nathatshjalpen.se/k/lagen/

Polismyndigheten. (3 juni 2024a). *Dataintrång*
https://polisen.se/utsatt-for-brott/polisanmalan/bedrageri/dataintrang/

Polismyndigheten. (3 juni 2024b). *Nakenbilder*.
https://polisen.se/utsatt-for-brott/polisanmalan/hat-hot-och-vald/nakenbilder/

Prins Carl Philips och Prinsessan Sofias stiftelse. (9 juli 2024). *Tryggare nätvardag*.
https://prinsparetsstiftelse.se/tryggarenatvardag/

Snapchat. (2024). How do I stay safe on Snapchat?
https://help.snapchat.com/hc/en-us/articles/7012304746644-How-do-I-stay-safe-on-Snapchat

Sveriges riksdag. (4 juli 2024). *Kränkande fotografering*.
https://www.riksdagen.se/sv/dokument-och-lagar/dokument/betankande/krankande-fotografering_h001juu21/

TikTok. (2024). Användarsäkerhet.
https://support.TikTok.com/sv/safety-hc/account-and-user-safety/user-safety

The eSafety Commissioner (eSafety) - Australia's independent regulator for online safety. (10 juli 2024). *Technology-facilitated abuse: family, domestic and sexual violence*.
https://www.esafety.gov.au/sites/default/files/2023-10/Technology-facilitated-abuse-family-domestic-sexual-violence-literature-scan.pdf

Ungarelationer.se. (8 juli 2024a). *Digitalt våld*.
https://ungarelationer.se/digitalt-vald/

Ungarelationer.se. (8 juli 2024b). *Om våld i relationer*. https://ungarelationer.se/category/om-vald/

Ungarelationer.se. (8 juli 2024c). *STÖDJA*.
https://ungarelationer.se/foralder-stodja/

Uppsala universitet, Nationellt centrum för kvinnofrid. (1 augusti 2024). *Ungas utsatthet för våld* https://www.uu.se/centrum/nck/kunskapsbank-om-vald/fakta-och-forskning-om-vald/ungas-utsatthet-for-vald

Åklagarmyndigheten. (1 augusti 2024a). *Ofredande*. https://www.aklagare.se/ordlista/o/ofredande/

Åklagarmyndigheten. (1 augusti 2024b). *Olaga förföljelse*. https://www.aklagare.se/ordlista/o/olaga-forfoljelse/

1177.se. (9 augusti 2024). Självkänsla. https://www.1177.se/liv--halsa/psykisk-halsa/sjalvkansla/

Det här är ett samarbete mellan

fredens hus

UPPSALA KVINNO JOUR

sentor
Part of Accenture

ctrl

ATT HA DEN ÄR LIKA VIKTIGT SOM ATT SLÄPPA DEN