TRYGGT PÅ WEBBEN

ANVISNINGAR FÖR FÖRÄLDRAR

2. UPPLAGAN

DITT DELTAGANDE ÄR MYCKET VIKTIGT!

PRODUKTION:

Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter har publicerat handböckerna på svenska.

Du kan beställa en pappersversion, komma med förslag eller meddela om fel per e-post till registrator@traficom.fi.

Handboken finns på kyberturvallisuuskeskus.fi/sv.

Originalverk: "Internet Segura"

Det ursprungliga verket producerades av CERT.BR och NIC.BR, det vill säga DE BRASILIANSKA MYNDIGHETERNA SOM ANSVAR FÖR INFORMATIONSSÄKERHET OCH DOMÄNNAMNET .BR, SAMT AV DEN BRASILIANSKA INTERNETSTYRGRUPPEN CGI.BR.

ALLMÄN KOORDINATION:

Cristine Hoepers

REDAKTÖR:

Miriam von Zuben

ILLUSTRATIONER:

Hector Gomez och Shutterstock

GRAFISK DESIGN OCH PUBLICERING:

Maricy Rabelo, Klezer Uehara, Giuliano Galvez

KORREKTURLÄSNING OCH ASSISTENTER:

André Lucas Fernandes, Caroline D'Avo, Evelyn Eisenstein (Rede ESSE Mundo Digital), Everton Teles Rodrigues, Fabiana Araujo, Helena Martins, Jorge Luiz Pinto de Souza (EMPREL), Leandro Morales B. Stefano, Marcelo H. P. C. Chaves, Maria Silvia Lordello Marques, Raquel Lima Saraiva, Rodrigo Nejm (Equipe SaferNet Brasil)

Tidigare versioner:
02/2017 – Första upplagan
10/2022 – Andra upplagan

SKYDDA DITT BARN.

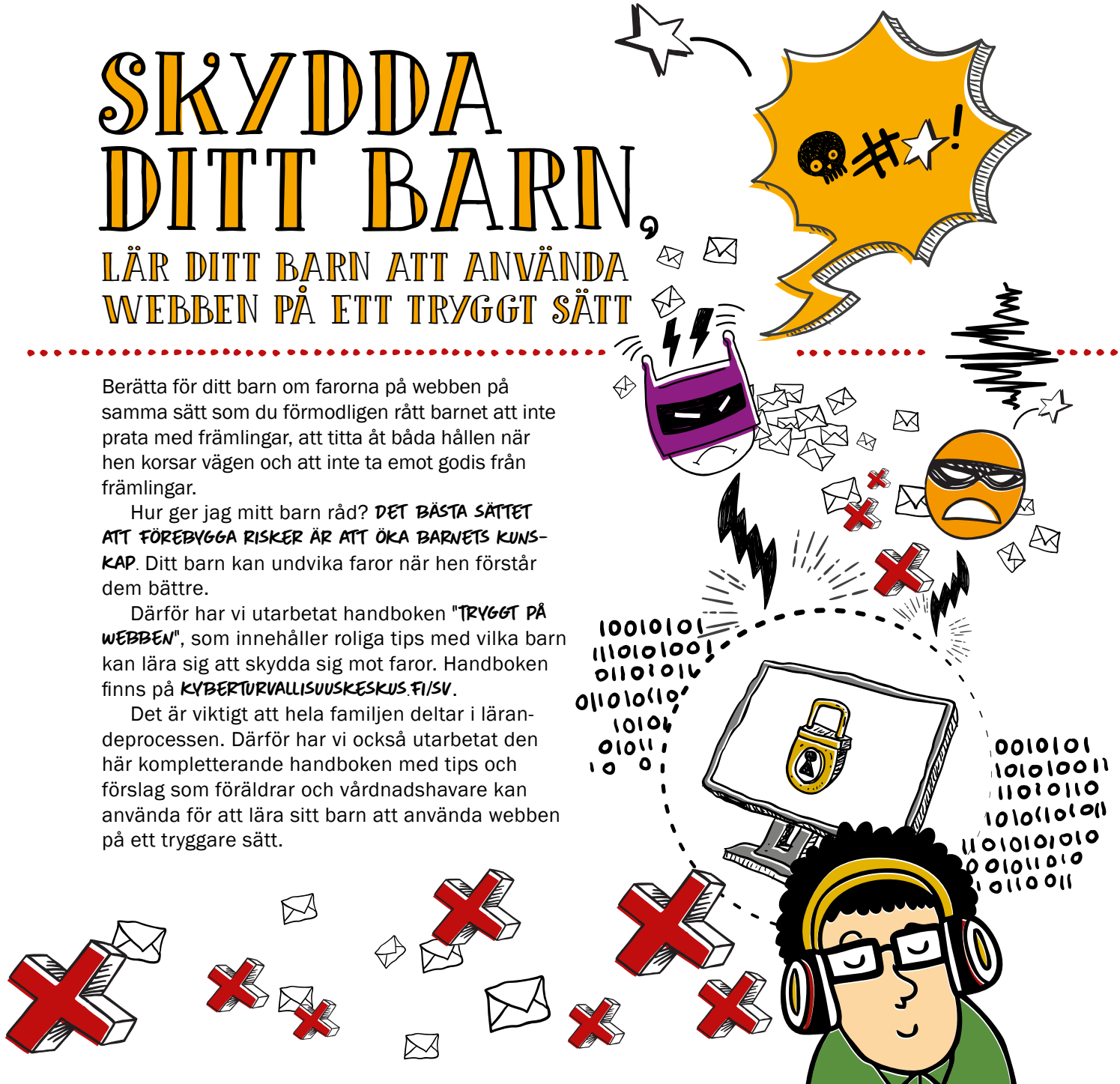
LÄR DITT BARN ATT ANVÄNDA WEBBEN PÅ ETT TRYGGT SÄTT

Berätta för ditt barn om farorna på webben på samma sätt som du förmodligen rått barnet att inte prata med främlingar, att titta åt båda hållen när hen korsar vägen och att inte ta emot godis från främlingar.

Hur ger jag mitt barn råd? **DET BÄSTA SÄTTET ATT FÖREBYGGA RISKER ÄR ATT ÖKA BARNETS KUNSKAP**. Ditt barn kan undvika faror när hen förstår dem bättre.

Därför har vi utarbetat handboken "**TRYGGT PÅ WEBBEN**", som innehåller roliga tips med vilka barn kan lära sig att skydda sig mot faror. Handboken finns på **KYBERTURVALLISUUSKESKUS.FI/SV**.

Det är viktigt att hela familjen deltar i läranderocessen. Därför har vi också utarbetat den här kompletterande handboken med tips och förslag som föräldrar och vårdnadshavare kan använda för att lära sitt barn att använda webben på ett tryggare sätt.



DET FINNS SKÄL TILL ATT KÄNNA RISKERNA

Fördelarna med internet är obestridliga och redan ganska välkända. Internet ger oss nya möjligheter varje dag, och vi vet att mycket ännu är på kommande.

Utan att glömma alla goda sidor som internet erbjuder ditt barn är det viktigt att komma ihåg att internet inte bara är en virtuell plats, utan dess användning innebär risker som du bör vara medveten om.

Överdriven internetanvändning kan äventyra ditt barns fysiska och psykiska hälsa, försämra hens framgång i skolan och påverka hens sociala liv.

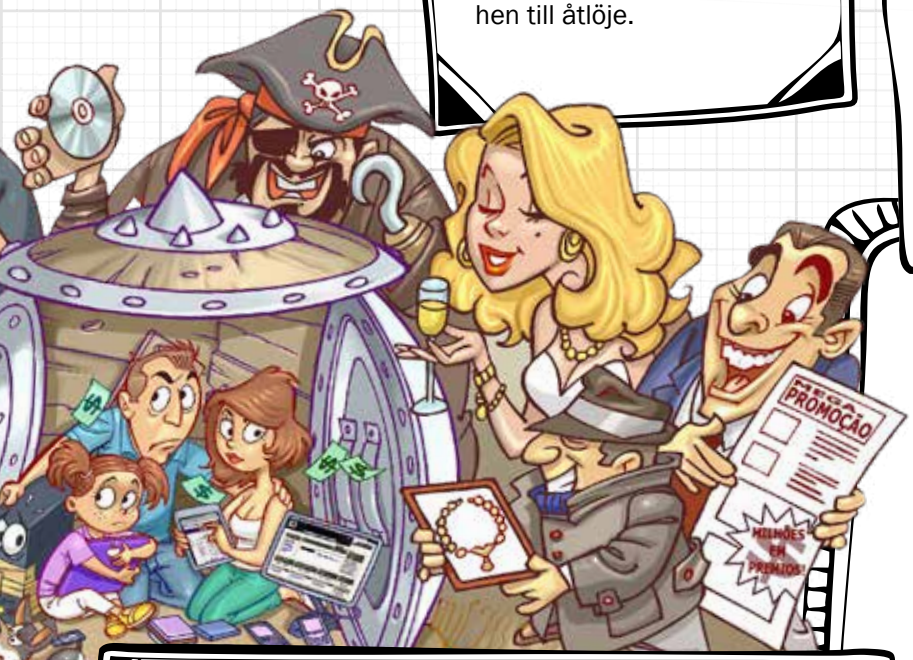
På webben kan ditt barn se olämpligt, falskt, bristfälligt eller kränkande innehåll, såsom skvaller, kedjebrev, porr eller våld. Att filtrera sådant innehåll kräver kritiskt tänkande, och beroende på åldern eller mognaden kanske ditt barn inte är redo för detta ännu.

Vissa utnyttjar internets skenbara anonymitet för att närma sig barn och begå brott mot dem, såsom sexuellt utnyttjande, utpressning, barnpornografi och kidnappning.

Om du sprider ditt barns personuppgifter kan det äventyra hens integritet. Dessutom kan barnet själv publicera information som äventyrar integriteten för hens familj och vänner.

Foton eller filmer på ditt barn kan bli virala fenomen, vilket snabbt kan göra hen till en ”internetkändis” och utsätta hen för extrem granskning samt även göra hen till åtlöje.

Saker som laddas upp på webben kan spridas snabbt och de är svåra att radera. Bilderna och videorna du tagit på barnet kan finnas tillgängliga ännu när hen har blivit vuxen.



Ditt barn kan utsättas eller anklagas för nätmobbning om hen publicerar, delar eller gillar foton, videor eller meddelanden på webben som generar eller skämmer ut hens skolkamrater.

Barns personligheter håller ännu på att formas och de är ännu inte mentalt mogna, vilket gör att de inte kan hantera kritik, avvisande eller missaktning från andra. Bilder som publiceras på barn kan skapa förväntningar på hur bilderna tas emot och det kan vara frustrerande för dem om bilderna inte ”gillas” snabbt eller om bilderna får negativa eller fördomsfulla kommentarer.

De apparater som ditt barn använder kan vara infekterade med skadeprogram, vilket kan leda till att data försvinner och tredje parter kan få obehörig åtkomst till exempelvis personuppgifter.

VAR INTE EN SKURK

EN DEL AV RISKERNA BARN MÖTER PÅ INTERNET BEROR PÅ ATT DERAS EGEN FAMILJ – VANLIGTVIS I GOD TRO OCH UTAN ATT KÄNNA TILL FARORNA – AVSLÖJAR FÖR MÅNGA SAKER OM DEM.

HAR DU REDAN SKAPAT EN PROFIL I DITT BARNS NAMN?

En del föräldrar skapar profiler i sina barns namn och publicerar ibland till och med saker så att det ser ut som om barnen själva publicerat dem. Det kan hända att barnet inte ens är fött men redan har en profil i sociala medier. Har du tänkt på hur det känns för barnet att läsa åsikter som hen inte framfört? Hur är det möjligt att i framtiden särskilja barnets egna publiceringar från sådana som publicerats av någon annan i hens namn?

KOM IHÅG ATT VISSA SOCIALA MEDIETJÄNSTER HAR FASTSTÄLLT EN MINIMIÅLDER FÖR ATT SKAPA ETT KONTO. Om inte ens föräldrarna som fungerar som exempel för barnen följer reglerna, hur ska de sedan kunna kräva det av sina barn?

BRUKAR DU PUBLICERA MEDDELANDEN OM DITT BARN PÅ WEBBEN?

Man behöver inte publicera saker på webben som är privata och bara rör familjen. Respektera ditt barns integritet, individualitet och intimitet. Barnet måste ha rätt att neka till publicering av saker som rör hen och att bygga sitt eget utrymme på internet när hens personlighet mognar och hen lär sig att använda olika teknologier.

Undvik att publicera meddelanden där du kallar barnet vid ett smeknamn som ni bara använder sinsemellan, eller där du behandlar hen som ett småbarn. Gräla inte och tillrättavisa inte barnet offentligt på webben. Diskutera saken med ditt barn innan du publicerar ett foto eller annat innehåll om er familj. Kom ihåg att internet är en offentlig plats och att man inte, som det gamla ordspråket säger, ska ”tvätta sin smutsiga byk offentligt”.

BRUKAR DU PUBLICERA BILDER OCH VIDEOR PÅ DITT BARN?

Har du redan stannat upp och funderat på i vilken utsträckning du har rätt att avslöja ditt barns privata angelägenheter? I vilken utsträckning har barnet rätt att förbjuda sina föräldrar att publicera saker om hen själv? Från vilken ålder har barnet rätt till sitt eget privatliv?

Saker som du tycker är ”gulliga” kan vara ångestframkallande för barnet och kan till och med användas för att mobba barnet. Kom ihåg att familjefrågor är privata angelägenheter.

Ett foto av ditt barn som badar eller leker på stranden naken eller halvnaken kan vara oskyldigt för dig, men pedofilnätverk kan använda samma foto för kommersiella ändamål relaterade till sexuellt utnyttjande av barn. **DELA ALLTSÅ INTE BILDER DÄR DITT BARN ÄR LÄTTKLÄTT**.

Om du berättar om barnets angelägenheter (studieplats, slutförda kurser och platser hen brukar besöka) kan det utsätta barnet för kidnappningsrisk. Utomlands har man i nyheterna rapporterat om många kidnappningar av barn som planerats med hjälp av information som erhållits i sociala medier. **UNDVIK ALLTSÅ ATT PUBLICERA BILDER SOM AVSLÖJAR VAR DITT BARN VANLIGEN RÖR SIG**.

Dessutom finns det ”digitala kidnappare” som använder barns riktiga uppgifter för att skapa falska profiler och diskutera med andra personer. I vissa fall kommenterar de till och med och delar bilder precis som om de var barnens riktiga föräldrar.

För att undvika dem ska du vara försiktig med **VILKA FRÄMMANDE PERSONER SOM DU GODKÄNNER I DINA SOCIALA NÄTVERK** och ställa in sekretessinställningarna för att begränsa vem som kan se dina publiceringar.

HJÄLP DITT BARN ATT SKYDDA SIG

DIN HJÄLP ÄR MYCKET VIKTIG. TA DEL AV NÅGRA TIPS OM HUR DU KAN LÄRA DITT BARN ATT ANVÄNDA WEBBEN PÅ ETT TRYGGARE SÄTT.

FÖREGÅ MED GOTT EXEMPEL

Föräldrarna är ofta de viktigaste förebilderna för sitt barn, så det är naturligt att barnen tillägnar sig sina föräldrars vanor och attityder. **DET HJÄLPER INTE ATT GE RÅD OM ATTITYDERNA INTE STÄMMER ÖVERENS MED DET MAN SÄGER.**

Fundera på om du surfar på webben medan du äter eller sneglar i sociala medier medan du pratar med ditt barn? Har du tid att skicka e-post även om du inte har tid att leka med ditt barn?

Kan du kräva ett visst beteende av ditt barn om du inte själv föregår med gott exempel? Ditt barn kommer förmodligen att agera på samma sätt som du.

TVEKA INTE ATT DISKUTERA

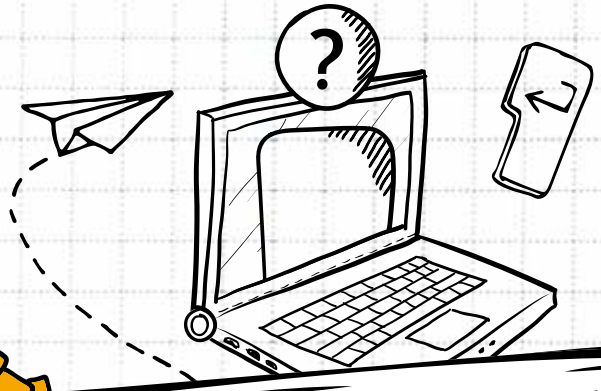
Det hjälper inte att förbjuda ditt barn att använda internet, eftersom hen kan använda det i hemlighet. Generellt sett skapar förbud konflikter och försvårar dialog. Var alltså närvarande i ditt barns liv, diskutera de olika möjligheterna som internet erbjuder med barnet och låt hen berätta om sina egna erfarenheter.

Hjälp också ditt barn att lösa de frågor som hen funderar på. På så sätt kan du visa att ni kan ha en öppen diskussion med varandra.

När du visar att du är intresserad av ditt barns angelägenheter är det också lättare för dig att upptäcka om barnet behöver hjälp, har ett problem eller är bekymrat över något. **DET KAN VARA MYCKET ROLIGT OCH LÄRORIKT ATT ANVÄNDA INTERNET TILLSAMMANS MED DITT BARN.**

Uppmuntra ditt barn att berätta om hen stött på obehagliga saker på webben. Du kan hjälpa hen med detta genom att berätta om olika exempelsituationer, hänvisa till problem som redan har inträffat eller genom att föra händelser på tal som varit i nyheterna och kommenterats allmänt. På så sätt kan du hjälpa hen att förstå problemen och ge akt på konsekvenserna. Samtidigt lär du ditt barn att agera rätt.

KOM IHÅG ATT EN UPPLYSANDE, ÖPPEN OCH ÄRLIG DIALOG ÄR DET BÄSTA SÄTTET ATT LÄRA DITT BARN ATT HANTERA DE UTMANINGAR HEN KAN MÖTA SOM MEDLEM I SAMHÄLLET.



UPPMANA DITT BARN ATT FÖRHÅLLA SIG FÖRSIKTIGT TILL FRÄMMANDE PERSONER

Internet för personer med långt avstånd mellan sig närmare varandra och hjälper till att stärka vänskapsband, men det möjliggör också kommunikation med okända personer. En del kan vara ute i goda avsikter, medan andra kan utnyttja den falska känslan av anonymitet som skapas på internet för att närma sig barn och begå brott eller trakassera barn.

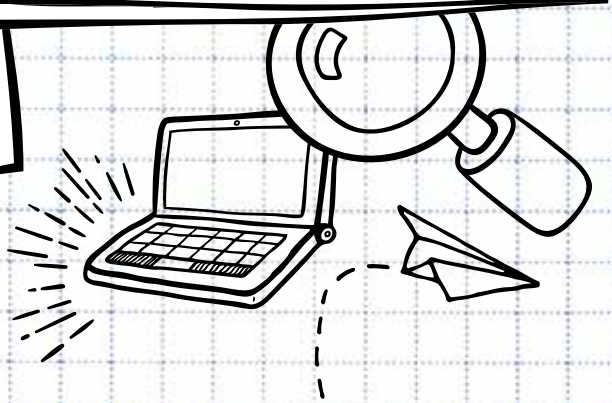
Tyvärr är det möjligt att vilseleda många barn, vilket leder till att de träffar människor som de inte känner personligen och därmed utsätts för stora faror utan sin vetskap. **LÄR DITT BARN ATT HEN ALDRIG SKA KOMMA ÖVERENS OM ATT ENSAM TRÄFFA PERSONER SOM HEN INTE KÄNNER ELLER SOM HEN BARA KÄNNER PÅ WEBBEN.**

IAKTTA DITT BARNS BETEENDE

Om ni har en dator hemma, förvara den på en plats där den är synlig. På det viset kan du iaktta vad ditt barn gör även på avstånd. Om barnet använder webben med sina egna apparater är det svårare att övervaka, men även då kan vissa tecken hjälpa dig.

Om ditt barn minimerar eller stänger appar, stänger dörren till rummet, skyddar mobiltelefonen eller surfplattan med ett eget lösenord eller är nervös när du är i närheten, kan det vara ett tecken på att hen försöker dölja något för dig och eventuellt är i fara. Om du upptäcker att ditt barn beter sig hemlighetsfullt på webben, be hen att berätta om det. Det viktigaste är ett förtroligt förhållande.

DISKUTERA OCH LYSSNA INNAN DU DÖMER, SÅ ATT DITT BARN INTE BEHÖVER VARA RÄDD FÖR ATT BERÄTTA OM SAKER OCH TING FÖR DIG.

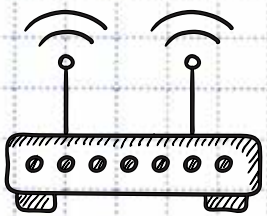


Berätta för ditt barn om integritet

Prata med ditt barn om vikten av att skydda integriteten och om att personlig information såsom hemmets och skolans adress inte ska delas på webben.

Instruera ditt barn i att välja vänner i sociala nätverk, och lär hen att inte godkänna personer som hen inte känner eller bara känner på distans som vänner. Hjälp ditt barn att justera sina profilinställningar så att publiceringarna är privata och endast hens vänner kan se dem. Barnet måste förstå att internet är en offentlig plats. Vännernas vänner kan också se, spara eller utnyttja information senare som publicerats på internet utan barnets vetskap.

Diskutera med ditt barn om att hen även ska skydda andras integritet. Barnet får inte ge ut information om var andra studerar eller arbetar eller vad de har köpt. Det är också bra att be om tillstånd innan man publicerar bilder eller videor där andra personer kan kännas igen.



När man talar om barnens integritet finns det skäl för att ta upp frågan om det är rätt att föräldrarna har barnens lösenord och att föräldrarna övervakar vad barnen gör.

Det finns inget entydigt och tydligt svar på den här frågan. När du själv var barn tyckte du förmodligen inte om att någon blandade sig i dina angelägenheter eller lyssnade på dina samtal, men å andra sidan var riskerna kanske inte lika stora som de är idag.

Som du säkert vet vinns förtroendet för föräldrarna småningom. Att tillåta ett barn att använda internet självständigt är som att ge barnet hemnyckeln – först vill föräldrarna inte ge nyckeln till barnet, sedan ger de den med olika instruktioner, tills de till sist ger nyckeln och inte oroar sig över saken längre.

Barns handlingar ska alltså övervakas kontinuerligt till en början, medan de med tiden och i takt med att de lär sig blir självständiga och kan lösa saker och ting på egen hand. När och hur denna övergång sker beror på varje barn och familj.

SE UPP FÖR NÄTMOBBNING

Symtomen hos nätmobbningsoffer är depression, dålig självkänsla, ångest, aggressivitet, rädsla och negativa känslor. Offren har också vanligtvis problem med att klara sig i skolan och undviker skolan.

VAR UPPMÄRKSAM OM DU SER SÅDANA TECKEN HOS DITT BARN OCH FÖRSÖK FRÅGA SKOLAN OM NÅGOT HAR HÄNT DÄR. Försök diskutera med ditt barn och uppmuntra hen att tala med någon annan som hen litar på, såsom ett äldre syskon, en farbror eller morbror, kusin eller lärare.

Om ditt barn gör sig skyldigt till nätmobbning kan du som ditt barns vårdnadshavare hållas ansvarig för det.

BERÄTTA FÖR DITT BARN HUR VIKTIGT DET ÄR ATT RESPEKTERA ANDRA MÄNNISKOR, så att barnet inte vidarebefordrar eller själv skapar innehåll som förödmjukar hens kompisar. Berätta också för ditt barn att även en lek har sina gränser och att det som hen själv tycker är på lek kan såra andra. Försök få hen att sätta sig in i offrets situation och fundera på om hen skulle gilla om någon gjorde samma sak mot hen.

RESPEKTERA ÅLDERSGRÄNSERNA

Många webbtjänster kräver en minimiålder av användarna. Man måste till exempel vara minst 13 år för att använda de flesta sociala medietjänster.

Om någon som är yngre än den åldersgräns som tjänsten kräver ljuger om sin ålder för att skapa ett konto, utsätts hen för olika risker. Barnet kan kontaktas med dåliga avsikter och kan komma åt innehåll som är olämpligt för hens ålder. Dessutom kan föräldrarna hållas ansvariga om något dåligt händer.

SÄTT REGLER

Sätt tydliga regler för internetanvändningen från början. Du kan till exempel tillåta användning av internet efter att läxorna är gjorda, endast på helger, några timmar om dagen eller under begränsade tider.

TÄNK PÅ ATT DET INTE HJÄLPER ATT SÄTTA MYCKET STRIKTA OCH OREALISTISKA REGLER, EFTERSOM DU INTE KAN ÖVERVAKA DEM HELA TIDEN. Även om du reglerar internetanvändningen med föräldrakontroll (se mer information nedan) kan barnen hitta vägar runt den, och samma begränsningar gäller inte för dem på andra apparater som till exempel i skolan eller hemma hos kompisar.

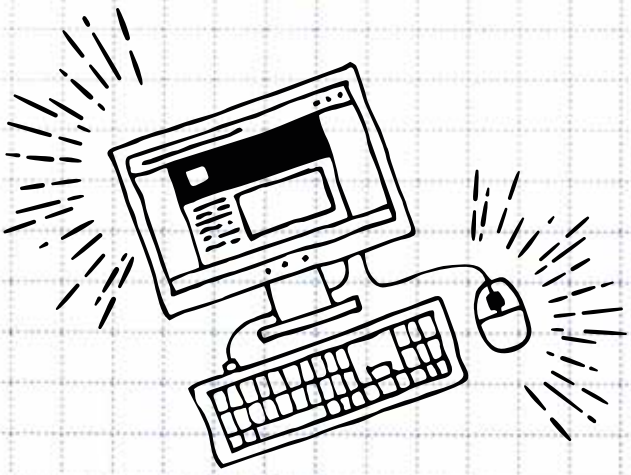
Därför är det viktigt att reglerna är överenskomna i förväg och att de är motiverade, respekterar barnets behov och skyddar hens fysiska och psykiska hälsa.

ANVÄND BARNLÅS

ÄVEN OM DET INTE FINNS NÅGON ERSÄTTNING FÖR DIALOG OCH FÖRÄLDRARNAS BEDÖMNINGSFÖRMÅGA, KAN TEKNIKEN ANVÄNDAS SOM EN MEDHJÄLPARE FÖR ATT SKYDDA BARNEN FRÅN FARORNA PÅ INTERNET.

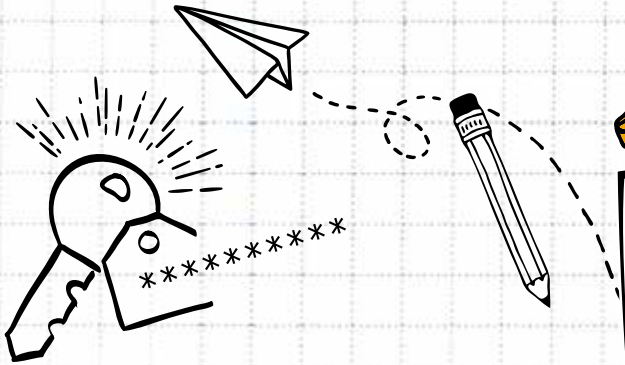
Barnlås avser olika säkerhetsfunktioner som kan användas i många olika operativsystem, på webbplatser och i apparater, såsom routrar och spelkonsoler. Barnlås kan också installeras genom att använda avgiftsbelagda eller gratis applikationer.

Säkerhetsfunktionerna för barnlås varierar beroende på hur de aktiveras. Exempel:



- **SÖKMOTORER:** I sökmotorerna kan du ställa in låsbara innehållsfilter som tar bort innehåll som är olämpligt för barn från sökresultaten.
- **OPERATIVSYSTEM:** Du kan begränsa vilka webbplatser barnen kan (eller inte kan) besöka, vilka appar som finns tillgängliga för barnen och med vem barnen kan kommunicera. Dessutom kan du sätta tidsgränser såsom en övre gräns för daglig användning, en gräns för läggdags och separata regler för vardagar och helger. Barnlåset förhindrar också lösenordsändringar och visar historikinformation om aktiviteter såsom besökta webbplatser och använda applikationer.
- **APPLIKATIONSBUTIKER:** Du kan bestämma en klassificeringsnivå (fritt eller enligt åldern) för appar som barnen kan köpa, ladda ner och installera. Du kan också begränsa vilka filmer som barnen kan se och vilka böcker de kan läsa i tjänsterna.
- **ANVÄNDAR- OCH PROFILSPECIFIKA BEGRÄNSNINGAR:** Du kan skapa begränsade konton för operativsystem och tjänster. Till exempel kan begränsade konton inte installera appar utan godkännande från ett annat konto.
- **ÄNDRINGAR I DNS[1]-SERVERN:** Du kan skaffa en DNS-tjänst som filtrerar tillåtna webbplatser på de apparater som används av barnen eller i hemnätverksroutern. De namnservrar som tillhandahålls av dessa tjänster har regler som hindrar åtkomst till webbplatser som är skadliga eller förbjudna för minderåriga och som kan innehålla till exempel pornografiskt innehåll.

[1] DNS (DomainName System) betyder domännamnssystem. Det omvandlar bland annat enhetsnamn och domännamn till IP-adresser och vice versa.



Det är viktigt att barnen inte känner till administratorslösenordet eller barnlåsets lösenord för sina apparater, så att de inte kan ta bort skyddet.

Även om barnlåset är ett ganska användbart verktyg **SKA DET ANVÄNDAS SOM ETT EXTRA SKYDD**. Barnlåset kan vara bristfälligt och finns nödvändigtvis inte på alla apparater och platser där barnen använder internet, såsom i skolan eller hemma hos kompisar. Det är därför en gammal god kontinuerlig dialog mellan föräldrar och barn är avgörande för att barnen ska känna igen farliga situationer och lära sig undvika dem.

SAMVETE OCH ANSVARSFULLT AGERANDE ÄR FORTFARANDE DEN ALLRA BÄSTA TEKNIKEN. Inget säkerhetsverktyg kan hjälpa dig att uppnå mognad och i synnerhet inte ersätta din egen försiktighet och ditt skydd. Detta gäller i allmänhet för livet i stort och därmed även internet, spel och applikationer.

HJÄLP DITT BARN ATT SKYDDA SINA ANVÄNDARKONTON.

Berätta för ditt barn hur viktigt det är att använda bra lösenord och att undvika lösenord som är lätta att gissa, såsom ”123456”, ”abcd”, ”asdf”, förnamn, efternamn, födelsedatum, hundens namn eller favoritlaget. Det lönar sig för barn att använda långa lösenord och börja använda tvåfaktorsautentisering.

Lär ditt barn att hen alltid ska logga ut från sina användarkonton när hen använder datorer som tillhör andra eller i gemensamma lokaler, som till exempel hemma hos kompisarna, på biblioteket och i skolan. På det viset kan nästa användare inte använda hens konton.

SKYDDA APPARATERNA SOM DITT BARN ANVÄNDER

De apparater som ditt barn använder kan infekteras av skadeprogram som kan äventyra lagrad eller angiven information, göra apparaterna långsammare eller hindra deras funktion. Därför är det viktigt att du ser till följande säkerhetsåtgärder:

- FÖRSÄKRA DIG OM APPARATERNAS SÄKERHET GENOM ATT INSTALLERA ALLA UPPDATERINGAR OCH LADDA NER DE SENASTE VERSIONERNA AV INSTALLERADE APPLIKATIONER.
- INSTALLERA SKYDDSMEKANISMER, SÅSOM ANTIVIRUSPROGRAM FRÅN EN VÄLKÄND TILLVERKARE OCH EN PERSONLIG BRANDVÄGG.

Vissa system har möjlighet till fjärrlokalisering. En sådan funktion kan vara användbar om apparaten tappas bort eller blir stulen. Användningen av fjärrlokalisering kräver att lokaliseringsdata aktiveras.

När man börjat använda lokalisering kan appar också använda barnets position och publicera lokaliseringsdata automatiskt. En del applikationer kan också begära onödigt omfattande rättigheter, till exempel rätt att använda kontaktuppgifter.

En del system gör det möjligt att till exempel begränsa användningen av lokaliseringsdata applikationsspecifikt. Säkerställ i inställningarna att applikationerna inte har onödiga rättigheter, och om det inte finns något begränsningsalternativ, leta efter alternativa applikationer som inte kräver lika omfattande användningsrättigheter.

HÅLL DIG UPPDATERAD

TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Utöver det här materialet hittar du en handbok avsedd speciellt för barn på kyberturvalliskeskus.fi/sv.

TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret