BASISSAK:

SIKKERHET

Mobiltelefoner, datamaskiner, apper og spill kan inneholde mye informasjon som barn bør holde trygg og privat. Heldigvis finnes det smarte grep for å beskytte seg selv fra svindel og kriminalitet. Her kan du lese fakta og råd om dette emnet.

TEKST: KRIS MUNTHE

Foto: New Africa / Shutterstock.com

Utvalgte fakta

Blant barn mellom 9-18 år:

- Halvparten har åpen bruker på Tiktok. (Generelt har 45-60 prosent privat bruker på sosiale medier).
- 7 av 10 har godtatt venneforespørsel fra noen de ikke kjenner fra før.
- 29 prosent kan passordet til foreldrene på Google Play eller App Store.
- 24 prosent har delt eget passord på sosiale medier med venner.

Og i tillegg, 44 % av foreldre bruker ikke foreldrekontroll på barnas enheter.

Kilde: Barn og Medier, 2020/Foreldre og Medier, 2020

Barnets mobiltelefon eller datamaskin er som en dagbok. Ikke er bare denne i seg selv en verdigjenstand, men den er også en nøkkel der alle installerte apper, e-posttjenester og andre programmer ligger åpne for bruk.

Derfor bør barnets enhet «låses» slik at uvedkommende ikke får adgang. I tillegg til de fysiske truslene – at noen stjeler mobilen til barna – opererer det også kriminelle på nett. For eksempel så kan det være tilfeller der noen får tak i barnets brukernavn og passord – endrer dette – og så låser barna ute fra en konto de har brukt lang tid på å bygge opp. Gode passord og bruk av totrinnsverifisering kan være med på å forebygge at det skjer.

Andre utfordringer kan gå på det økonomiske dersom barna kjøper innhold eller trykker på lenker til dyre abonnementstjenester. Her kan både hundre- og tusenlapper trekkes fra bankkortet. Ved å ha egne barnebrukere med sperrer for kjøp og ved å sette opp kostnadssperrer på mobilabonnementet til barna, kan man forebygge slike, ubehagelige overraskelser.

Man bør også velge gode personverninnstillinger slik at man begrenser publikummet som barna når ut til på sosiale medier og i spill. Ubegrenset chat med fremmede kan være stikkveier til overgrepssituasjoner og annen type uønsket kommunikasjon. Og selv om all verdens innstillinger ikke er en helgardering mot risiko på nett – kan det allikevel redusere på omfanget av utfordringer.

Sist, men ikke minst, er det en del skadelig programvare og lenker som leder til svindelsider. Ved å holde apper og enheten oppdatert, og ved å øke barns bevissthet rundt det å unngå å trykke på tvilsomme lenker og være kritiske til bruk av offentlige nettverk – kan man unngå noe av dette.

Barnevaktens råd til foreldre

- Gi barna en egen «barnebruker» som du som forelder administrerer.
- Bruk skjermlås.
- Velg sikre passord i sosiale medier, spill og andre tjenester.
- Slå på totrinnsverifisering.
- Last ned oppdateringer til mobiltelefon og apper jevnlig.
- Vær obs på bruk av offentlige nettverk.
- Se gjennom personverninnstillinger.
- Lær barna å ta skjermbevis.
- Rapporter hacking, spam og nettkriminalitet.

Foto: Mother_ana / Shutterstock.com

Gi barna en egen «barnebruker»

Enten det er en datamaskin eller mobiltelefon – kan man opprette egne barnebrukere. Da kan man som forelder sette sperrer for pengebruk, hvilke apper og spill barna kan laste ned, hvilke nettsider barna kan besøke, og man kan begrense funksjoner som kamera, GPS-plassering, kontaktlister og mer.

I disse tilfellene blir altså foreldrene «sikkerhetsekspertene» på vegne av barna. Ved å stenge for nedlasting av apper og visse nettsider – kan man begrense omfanget av tvilsomme apper som kan lastes ned.

Slik setter du opp «barnebrukere»:
iOS: Via skjermtid-funksjonen
Android: Via Family-link appen
Windows: Via Microsoft familie-gruppe
Spillkonsoller: Les mer på vår samleside

- Tips: Har barnet eget mobilabonnement? Påse at dette er registrert på barnets navn. Og sett opp sperre for overforbruk av mobildata, spesialnumre, innholdstjenester og utenlandssamtaler

Råd til barn

- Bruk skjermlåsen som foreldrene har satt opp for deg
- Velg sikre passord i sosiale medier, spill og andre tjenester
- Ikke del passordene dine med andre
- Slå på totrinnsverifisering, få hjelp av en voksen om du ikke vet hvordan du gjør dette
- Lag private brukere på sosiale medier hvis du bare vil at venner skal se innholdet du deler
- Ta skjermbevis av trakassering, plaging eller annen type kriminell oppførsel
- Si ifra til foreldre eller en voksen du stoler på dersom noe kriminelt skjer på nett!
- Bruk rapporteringsmulighetene som finnes på sosiale medier og i spill
- Bare bruk trådløse nett som du stoler på, ikke del privat informasjon på offentlige nettverk

Lag en skjermlås

Å låse en mobiltelefon eller en datamaskin med en kode – hindrer andre fra å logge inn og snoke dersom de fysisk får tak i enheten. Ofte er man allerede logget inn på forskjellige sosiale medier og e-posttjenester som ligger åpne når enheten er åpen.

Det finnes forskjellige former for å låse enheten – det kan være ved bruk av fingeravtrykk, ansiktsgjenkjenning eller en kode man taster inn. Det foregår diskusjoner om hvor sikker ansiktsgjenkjenning egentlig er (lure kameralåsen med et bilde).

Slik setter du opp en skjermlås:
iOS: innstillinger > Face ID og kode
Android: innstillinger > sikkerhet og posisjon > skjermlås
Windows: innstillinger > påloggingsinnstillinger

- Tips: Apple produkter har en innstilling som sletter all data på enheten etter ti mislykkede forsøk. Dette er et ekstra lag med sikkerhet slik at «tyvene» ikke får uendelig med forsøk. Pass på å sikkerhetskopier enheten jevnlig, slik at man ikke mister data på denne måten.
- Tips: Velg en kode som er vanskelig for andre å gjette (ikke bruk bursdag, postnummer, årstall og lignende)
- Tips: Sett skjermlåsen til å slå seg på så raskt som mulig etter bruk
- Tips: Dersom enheten blir stjålet har både Google og Apple funksjoner for å låse enheten eksternt, eller for å slette data
- Slå derfor på «hvor er» på Apple produkter og Android

Velg gode personverninnstillinger

Mange apper og spill har gode personverninnstillinger som kan påvirke hvem som ser innhold man legger ut og hvem som kan kontakte deg. Det er alltid lurt å ta et blikk på hvilke muligheter som finnes for å begrense dette.

- Tips: Gjør gjerne kontoen «privat» på sosiale medier slik at ikke alle kan se innholdet du legger ut.
- Tips: Om mulig, begrens mulighetene for private meldinger til kun venner
- Tips: Se over om profilen din er synlig for andre – og ikke skriv inn personlig informasjon her som adresse, ekte navn, skole osv.
- Tips: Vær obs på hvem man deler bilder med. Er det bedre å velge «venner» og ikke «offentlig/alle»?

Slå på totrinnsverifisering

Totrinnsverifisering bør være obligatorisk å bruke i alle apper, sosiale medier og spill. For hver pålogging på en tjeneste som ikke er på den enheten man bruker til vanlig – kreves en unik kode som blir sendt til mobiltelefon eller e-post.

Selv om noen får tak i barnets brukernavn og passord, kan de ikke logge inn uten denne unike koden. Man kan som regel velge å få koden tilsendt på SMS, e-post eller gjennom en godkjenner-app.

- Tips: Kjært barn har mange navn, og totrinnsverifisering kan også ha andre titler som for eksempel «multifaktorautentisering» eller «flefaktorautentisering». Prinsippet er uansett det samme

Les mer om hvordan du konkret går frem for å slå på totrinnsverifisering i populære apper og spill.

Ressurser

For foreldre:

- Barnevaktens samleside om smarte innstillinger.
- Ved kjøp i apper og spill/netthandel/mobiltjenester – Forbrukerrådet.
- Ved mistanke om eller brudd på lovverk kontakter man politiet direkte. Man kan også sende inn generelle tips.
- Ved uventede trekk fra bankkontoen eller bekymring for kontoopplysninger bør man kontakte nettbanken.
- Ved utgifter som angår mobilabonnementet bør man kontakte mobiloperatøren sin.
- Ved bilder og innhold som har blitt delt videre uten din tillatelse/hjelp til å slette kontoer – Slettmeg.no.
- Ved kontoer som er blitt hacket/tapt på sosiale medier og spill bør man kontakte tjenestetilbyderen direkte.
- Gratis nettvett-kurs fra nettvett.no.

For barn:

- Barnevaktens episode om nettsikkerhet for elever.
- Dubestemmer.no – lær om personvern, nettvett og digital dømmekraft.

Bruk sikre passord

Alle sosiale medier og kontoer på spill og e-post bør sikres med gode passord. **Det viktigste er at passordene er lange, men samtidig mulig å huske!** Man bør snakke med barna om å holde passord privat.

Norsis gir disse rådene for å lage gode passord:

- Lag så lange passord som mulig.
- Ha ulike passord for hver konto.
- Bruk tall, symboler og små/store bokstaver.
- Ikke bruk ord eller tall som kan assosieres med deg eller tjenesten passordet gjelder for.

Norsis advarer også mot at man bruker «husk passord» – funksjonen. Mange nettlesere foreslår å huske passordet til neste innlogging. Men dette er ikke en sikker løsning.

«Husk innlogging» derimot (at tjenesten husker at du har logget inn tidligere) utgjør ikke samme risiko for at andre stjeler passordet.

Man kan gjøre passordjobben lettere ved å bruke programmer som husker og lager passord for deg.

For eksempel så har Apple en passordgenerator (nøkkelring) som forslår og skriver inn sterke passord på forskjellige tjenester. Google har noe av det samme med «Smart Lock».

Norsis sier at man gjerne kan bruke passordhåndteringsprogram, så lenge disse er låst med en dobbelsikring (hovedpassord).

- Tips: Bruk en frase eller en setning for å lage et passord som er enkelt å huske. For eksempel «Jeglikerpizzabrusogtaco28».
- Tips: Noen tjenester sier selv ifra om passordet ditt er sikkert nok ved registering av ny konto.
- Tips: Ved mistanke om at noen andre har fått tilgang til kontoen din – bytt passord.

Forskning, rapporter og lenker

Her finner du relevante kilder og datamateriale som gir innblikk i emner om barn og unges sikkerhet på nett.

- Medietilsynets undersøkelser om barn og unges medievaner: Barn og Medier, 2020
- Medietilsynets undersøkelser om foreldres regulering av barnas mediebruk: Foreldre og Medier, 2020
- EU Kids Online 2020
- Norsis: Ungdom og digital sikkerhetskultur, 2017

Last ned sikkerhetsoppdateringer jevnlig

Ved jevne mellomrom dytter Apple, Google og Windows ut systemoppdateringer til enhetene sine. Disse inneholder oppdateringer som blant annet gir bedre sikkerhet. Som regel ordner datamaskinen eller mobiltelefonen opp i dette selv ved å holde seg oppdatert.

Men man kan alltids ta en sjekk inne i innstillinger og manuelt se etter oppdateringer i ny og ne. Det er også viktig å holde appene som barna bruker oppdatert.

På en Windows-PC bør man slå på brannmur og virusprogram. Man kan bruke den løsningen som allerede finnes i Windows. På mobiltelefoner og nettbrett er på sett og vis denne sikkerhetsløsningen bygget inn i enheten. Selv om det finnes egne antivirus-apper som man kan laste ned i tillegg.

- Tips: Vær kritisk til apper og programmer som du laster ned. Er kilden/nettsiden/eieren av appen til å stole på? Google og Apple sjekker gjennom appene i butikkene sine, men også her har det oppstått utfordringer tidligere.
- Tips: Se over hvilke tillatelser apper ber om. Er det riktig at appen skal få lov til å bruke GPS, kontaktlisten på telefonen, mikrofon osv? Stemmer det overens med appens formål?
- Tips: Vær kritisk til lenker som dukker opp på e-post. Svindlere kan opprette imitator-sider som ligner på alt fra sosiale medier til nettbanken din.
- Tips: Vær kritisk til lenker og uvanlige meldinger (rar måte å henvende seg på) fra venner på sosiale medier og i spill. Det kan hende at venner har fått kontoen hacket og at svindlerne gjennom dem sender lenker med virus/falsk innlogging.

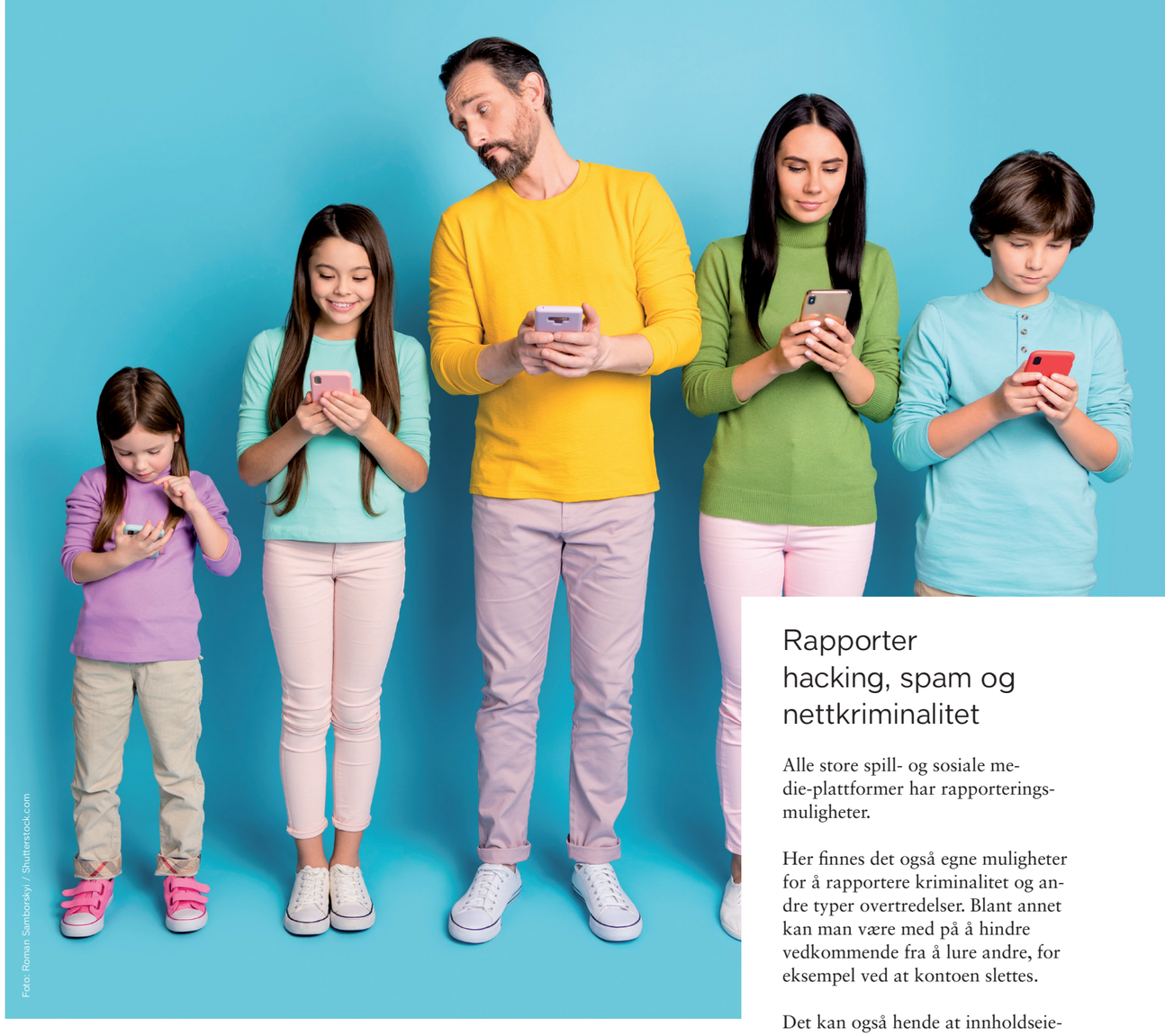

Foto: Roman Samborskyi / Shutterstock.com

Vær obs på offentlige nettverk

Det er forskjell på det å koble seg til hjemmenettverk og mobildata sammenlignet med offentlige nettverk på restauranter og kjøpesentre. Generelt kan man si at sistnevnte gir dårligere sikkerhet – der uvedkommende potensielt kan få tilgang til trafikken på mobiltelefonen din.

Så dersom det er sensitiv data – nettbank og lignende – kan det være lurt å gå over på mobildata og ikke offentlige nettverk. Er man enda mer viderekommen, kan man bruke VPN-løsninger – som sikrer informasjonen fra avsender til mottaker.

- Tips: Noen mobiltelefoner tilbyr deling av internett. Så man kan bruke barnas nettbrett eller en datamaskin og «låne» mobildata fra mobiltelefonen.

Rapporter hacking, spam og nettkriminalitet

Alle store spill- og sosiale medie-plattformer har rapporteringsmuligheter.

Her finnes det også egne muligheter for å rapportere kriminalitet og andre typer overtredelser. Blant annet kan man være med på å hindre vedkommende fra å lure andre, for eksempel ved at kontoen slettes.

Det kan også hende at innholdseieren får logget bevis eller annen type informasjon kan være nyttig ved lovbrudd og politietterforskning.

Ta skjermbevis

Dersom noe kriminelt har oppstått på internett kan det være lurt å ta bilde av skjermen som bevis. For eksempel av chat og bilder som blir delt ved mistanke om at noe kriminelt har oppstått. Dette kan gjøres både på mobiltelefon og datamaskin.

Se fremgangsmåte her.