



Internett-sikkerhet for familien

En praktisk veiledning som viser hvordan familien kan være sikker på Internett

Hans Peter Østrem

Norton
from symantec

Innledning

Internett er et fantastisk og mangfoldig sted, fullt av utrolige informasjonskilder og bokstavelig talt millioner av muligheter for å treffe nye venner og bli kjent med Internett-miljøer. Men for mange foreldre og foresatte som ofte har lite kunnskap om og erfaring med Internett, kan dette være et sted som de ser på med usikkerhet og bekymring. Vi er bekymret for hva eller hvem våre barn treffer på Internett, og hvordan vi kan beskytte dem med vår begrensede kunnskap.

Barna har vokst opp med all denne utrolige teknologien som vi ikke kunne drømme om da vi var barn. For dem er Internett bare ett av de stedene de bruker til å kommunisere, å leke og lage ting, eller et sted hvor de er sammen med sine venner. Det er viktig at vi balanserer våre bekymringer om barnas Internett-sikkerhet med deres mulighet for å utforske nettet, og at de kan gjøre dette i visshet at de kan komme til oss hvis de opplever noe ubehagelig eller forvirrende på nettet.

Mange stiller spørsmål som disse:

- Hvordan kan jeg være sikker på at mine barn ikke snakker med fremmede?
- Hvor gamle bør mine barn være før jeg lar dem opprette en sosial nettverksside?
- Hva skal jeg gjøre hvis jeg har mistanke om at barnet mitt blitt nettmobbet?

Dette er viktige spørsmål, og foreldre trenger først og fremst hjelp med å forstå nye applikasjoner som sosiale nettverkssider og direktemeldingsprogrammer og risikoen forbundet med disse. Men de må også få en forståelse for de positive sidene og de mulighetene som Internett-tilstedeværelse gir, og hvordan de kan engasjere seg mer i barnas Internett-tilværelse. Som selskap tilbyr Symantec en rekke produkter som holder datamaskinen sikker. Men det er avgjørende at du samtidig som du beskytter maskinen mot trusler som virus og hackere, også tenker på barnas sikkerhet. Det er her dette heftet kan være til hjelp. Det inneholder verdifulle råd i forbindelse med de Internett-miljøene som er populære med barn i bestemte alderstrinn, og tilbyr praktisk støtte.

Min rolle som talsperson for Internett-sikkerhet handler om å gi både foreldre og barn de forutsetninger som skal til for å få mest mulig ut av Internett på en sikker og trygg måte. Dette heftet er en begynnelse på en spennende utvikling, hvor du og barna kan lære og utvikle dere sammen. Jeg vil fortelle om de mest populære stedene på Internett og nye trender, og nevne hvor man bør være på vakt og anbefale hva som bør gjøres for å beskytte barna i slike situasjoner.

Enten dine barn først er begynt å bli kjent med Internett, eller du har tenåringer som har utviklet en fascinasjon for sosiale nettverkssider, så er mitt beste råd at du ikke må være redd og i stedet for lære sammen med dine barn og rådføre deg med dette heftet.

Hans Peter Østrem
Nortons talsperson for Internett-sikkerhet
www.norton.com/no/familyresource



Innhold

De forskjellige alderstrinnene	4
Barn i alderen 5–7 år	4
Barn i alderen 8–12	5
Tenåringer (13–17 år)	6
Høyere utdanning og deretter	8
Følg reglene	9
Foreldre	9
Barn og ungdom	10
Grunnleggende	11
Sikker nettsurfing	11
Beskytt ditt passord	11
Sikre ditt trådløse nettverk	12
Foreldrekontrollprogramvare	12
Internett-favoritter	13
Risiko	14
Overgripere på Internett	14
Plagiat og lureri	14
Nettmobbing og nettforfølgelse	15
Deling av filer, musikk og video	15
Tyveri av identitet og informasjon	16
Sosiale nettverkssider	16
Porno, spill, rasisme, anoreksi og hat på nettet	17
Online privatliv for tenåringer	17
E-post og direkte meldinger	18
Blogging	19
Virus, ormer og spionprogrammer	20
Bot på alvor	20
Digitale bilder	21
Internett-handel	21
Betaling av regninger på Internett	22
Nettbanktjenester	22
Internett-spill og tegn på avhengighet	22
Noen ord avslutningsvis	23
Gode råd for beskyttelse av familien på nettet	23
Viktige ressursider	24



De forskjellige alderstrinnene

Barn i alderen 5–7 år

Dette er alderen hvor mange barn blir kjent med Internett. Nå som skolene har både datarom og datamaskiner i klasserommet, er det ofte på skolen barn først lærer å bruke en datamaskin. Men mange blir kjent med datamaskinen i hjemmet, hvor de lærer av foreldre eller eldre søsken. Småbarn blir ofte oppslukt av enkle spill og undervisningssider, men de vil fort lære om nye webområder av sine venner. Småbarnsforeldre bør slå av slike funksjoner fra begynnelsen av. Det er vanskelig for barn i denne alderen å forstå farene som er forbundet med at noen kontakter dem via vennligsinnede brukergrensesnitt på en spillside eller medlemside. Senere kan du lære dem hva chattefunksjonen er for noe, ved at dere chatter med familie og venner, og sørge for at barna lærer alltid å be om lov til å chatte med noen på nettet.

Det beste ville være at du involverer deg like mye i barnas Internett-aktiviteter som i deres hjemmelekser. F.eks. bør du sørge for at datamaskinen barna bruker, er innenfor synsvidde og er satt opp i familiens oppholdsrom. Det er en god ide å velge en barnevennlig nettportal som datamaskinens hjemmeside og vurdere å legge inn bokmerker for et utvalg webområder som du ikke har noe i mot at barna besøker. Vis dem hvordan de kan få tilgang til dem i Favoritter-mappen, som du kan gi barnas navn.¹ Foreldrekontrollprogrammer kan hjelpe deg med å begrense hvilke sider barna kan få adgang til, selv når du ikke er til stede. Kontrollmekanismen blokkerer all informasjon som du ikke ønsker at barna skal dele, enten det er deres

¹ For begge disse tjenestene kan du klikke på Verktøy-knappen på nettleserens menylinje

navn, alder, telefonnummer eller andre private data. Du bør slå på alle filter- og sikkerhetsfunksjonene i datamaskinen for å unngå att barna tilfeldigvis kommer inn på en side med upassende innhold. Vis barna hvordan de lukker et vindu i nettleseren, og forklar dem at det alltid er i orden å lukke en side hvis noe overraskende eller truende skjer. Si dem at de aldri må chatte, skrive meldinger eller dele informasjon med noen hvis ikke dere som foreldre er til stede.

Viktige anbefalinger:

- Begrens godkjente webområder og antall timer barna er på Internett.
- Innstill sikkerheten til høy på nettlesere, medlemskap og sosiale nettverkssider.
- Installer og vedlikehold Internett-sikkerhetsprogrammer og foreldrekontroll.
- Bruk foreldrekontroll til å begrense utvalget av webområder som barna kan besøke.
- Overvåk barnas bruk av datamaskinen, og sitt sammen med dem når de er på Internett, når det er mulig.
- Forklar at det er viktig å beskytte privat informasjon (navn, telefonnummer osv.), og at de aldri må dele passord med venner eller noen andre.

Barn i alderen 8–12

Denne aldersgruppen er mye mer sosial og utforskende i deres bruk av datamaskinen. De snakker med venner på skolen og lærer hva som er siste nytt og de kuleste sidene. Dette er alderen hvor mange registrerer sin første e-postadresse og direktemeldingskonto. Spør ditt barn om disse kontoene og hva deres passord er, slik at du kan overvåke deres aktiviteter og vite hvem de kommuniserer med. Barn i denne alderen kan også besøke sosiale nettverkssider som MySpace, Piczo og Bebo, som er populære blant eldre tenåringer og voksne. De fleste vil ikke selv opprette en side før de er blitt litt eldre, men de vil gjerne besøke og chatte med venner, eldre søsken og andre medlemmer av familien som har slike sider og profiler.

Denne aldersgruppen er også interessert i musikk, og Internett gjør det enkelt å lytte, oppdage og laste ned nye låter samt å møte andre som deler deres musikksmak. Kanskje de ser etter nyheter om favorittband eller kjendiser og besøker deres blogger og webområder, eller sjekker ut forskjellige sider for å få siste nytt fra ryktebørsen og laste ned bilder. Internett-videosider, som YouTube, er enormt populære. Mange

av videoene inneholder kraftig språkbruk og voldelig materiale, så det er nødvendig at du overvåker dine barns besøk på slike sider. Noen av de mer kreative i denne aldersgruppen, lærer hvordan de skal ta digitale bilder, redigere video og dele arbeidene sine med venner og familie. Med din hjelp, eller med hjelp fra mer erfarne venner, begynner de også å laste opp det de har laget, til Internett.

Viktige anbefalinger:

- Sjekk jevnlig datamaskinens logg for å se hvilke sider barna har besøkt, og overvåk deres kontoer for e-post og direktemeldinger for å se hvem de kommuniserer med. La barna få vite at du gjør dette, slik at de ikke mister tilliten til deg.
- Opprett et sett med regler om Internett-kommunikasjon, Ulovlige nedlastinger og nettmobbing.
- De må vite at de aldri skal klikke på en kobling i en e-post eller direktemelding, fordi dette er en vanlig måte å få virus eller røpe private data til kriminelle.
- Diskuter risiko og farer ved å laste opp og dele privat informasjon, videoer og fotografier.
- Se etter tegn på overdreven Internett-atferd eller -avhengighet (se avsnittet "Internett-spill og tegn på avhengighet").
- Plasser datamaskinen i boligens oppholdsrom.
- Oppretthold åpen kommunikasjon og oppmuntre barna til å fortelle om ting som de opplever på Internett, og som de synes er ubehagelige.

Tenåringer (13–17 år)

Tenåringer utvikler mer og mer sin uavhengighet, og dette kan også sees i deres Internett-tilværelse. Med uavhengighet kommer ansvar, inkludert det å være forsiktig på Internett. I denne alderen har tenåringer vanligvis opprettet eller blitt medlemmer av nettsamfunn som MySpace, Facebook, Bebo og andre. Med brukernavn, medlemskap, blogger, profiler og andre Internett-elementer som de besøker daglig, kommuniserer tenåringer informasjon om sine liv med hverandre. Webområder er også ofte brukt i forbindelse med lekser og innlevering av oppgaver. De kan etterlate seg digitale spor om sine tanker og aktiviteter over alt på nettet. Ofte vet de ikke, eller de glemmer, at alt som de laster opp på nettet, kan ses av alle og trolig vil forbli der ute til evig tid. Alt som kreves, er et enkelt søk på Google™ fra

potensielle arbeidsgivere eller representanter fra institusjoner innen høyere utdanning om fem, ti, tjuer år fra nå, og så vil alle bildene, meningene og tankene fra tenåringsalderen dukke opp i treffet. Forsiktighet er viktig!

Viktige anbefalinger:

- Forsterk reglene for passende Internett-atferd (språk, privat informasjon og bilder, nettetikk, ulovlig nedlasting, begrenset antall timer på nettet og å ikke gå inn på upassende sider).
- Vær oppmerksom på dine tenåringers aktiviteter på nettet (sosiale nettverkssider, bilder, privat informasjon, klubb- og sportsaktiviteter), enten det er på deres egne sider, venners sider eller på skolens websider.
- Vurder de webområdene som dine tenåringers besøker, og ikke vær redd for å diskutere og forby webområder som du mener er upassende.
- Forklar dem at de ikke må laste ned filer uten din tillatelse (musikk, spill, skjermspare, ringetoner osv.).
- Forklar dem at de aldri må dele passord og være forsiktig med hvilke private data de gir fra seg når de er på en delt eller offentlig datamaskin, eller hvis de tror maskinen de bruker, ikke er sikker.
- Lær dem at de aldri må klikke på en kobling i en e-post eller direkte melding, fordi dette er en vanlig måte å få virus eller røpe private data til kriminelle.
- Plasser datamaskinen i boligens oppholdsrom og ikke på tenåringens soverom.
- Fostre åpen kommunikasjon, og oppmuntre tenåringene til å fortelle om ting som de kanskje opplever som ubehagelige på Internett. Husk at selv om de er tenåring, har de fortsatt bruk for din støtte og omsorg.
- Minn tenåringene på at de har ansvar for vedlikehold av Internett-sikkerhetsprogrammene og oppdateringer, og at dette er for deres egen sikkerhets skyld.

Høyere utdanning og deretter

Etter hvert som tenåringene vokser opp og forlater hjemmet, enten til videre utdanning eller arbeid, er det viktig at de er kjent med det ekstra ansvaret de som voksne har når de befinner seg på Internett. Det inkluderer beskyttelse av eget privatliv, spesielt økonomiske data, forebygging mot identitetstyver, relatert til fremtidig kredittverdighet. Dette er spesielt viktig for unge voksne. Hvis dine tenåring benytter en bærbar datamaskin på skolen eller i arbeid, må du sørge for at de forstår den ekstra risikoen som er forbundet med bruk av trådløse forbindelser, og at de må kryptere slike forbindelser og kjøpe det nødvendige sikkerhetsutstyret og pålitelige sikkerhetskopier. Kanskje de føler seg fristet til å hoppe over disse ekstra produktene, så det er viktig at man insisterer når det gjelder sikkerhet på bærbare datamaskiner.



Følg reglene

Foreldre

Husk disse viktige rådene når det gjelder sikkerhet på nettet:

- Vær aktivt interessert i dine barns aktiviteter på nettet.
- Husk at barna kobler seg til nettet på skolen, i venners hjem, på biblioteket, på Internett-kafeer osv.
- Oppmuntre barna til å komme til deg med ting som de finner ubehagelige på nettet.
- Minn dine barn om at de aldri må gi fra seg personlig informasjon.
- Barn bør aldri møte noen ansikt til ansikt som de har truffet på Internett, uten at de går sammen med en voksen som er til å stole på.
- Oppmuntre barna til å bli ansvarlige Internett-brukere.
- Hold dere til de morsomme og positive sidene på Internett.
- Du må ikke tro at du er alene om dette. Her er noen webområder som kan hjelpe deg:

www.nettvett.no

www.saftonline.no

www.reddbarna.no

www.barnevakten.no

www.tryggsurf.no

Barn og ungdom

Overhold **SMART**-reglene

Smart – Sikker. Vær forsiktig med hvem du gir ut personlig informasjon til, som navn, e-postadresse, telefonnummer, hjemmadresse eller skolenavn. Gi dem aldri til folk du bare kjenner fra Internett.

Meeting – Å møte noen ansikt til ansikt som du har truffet på nettet, kan være farlig. Dette må du kun gjøre hvis du har tillatelse fra dine foreldre eller dem som har ansvaret for deg, og de bør alltid være med deg. Du må aldri gå alene.

Accepting – Å akseptere e-poster, direktemeldinger eller å åpne filer, bilder eller tekster fra folk som du ikke kjenner eller kan stole på, kan føre til problemer – de kan inneholde virus og ubehagelige meldinger.

Reliable – Pålitelig. På Internett kan man alltid lyve om hvem man er, og informasjon som du finner på Internett, kan være upålitelig.

Tell – Fortell dine foreldre eller andre voksne som du kjenner, hvis det er noe eller noen på Internett som du synes er ubehagelig.



Sikker nettsurfing

Sørg for at nettleseren din er innstilt slik at innebygde sikkerhetsfunksjoner er aktivert. F.eks. tilbyr Microsoft Internet Explorer (den mest populære nettleseren) innstillinger for sikkerhet og personvern. Disse finner du under "Alternativer for Internett" på "Verktøy"-menyen.

Beskytt ditt passord

Unngå å bruke passord som det er lett å gjette seg til, som ord fra ordbøker, navn eller datoer, som din fødselsdato, som både dine barn og hackere kan finne. Her er en god måte å håndtere passord på: Velg et masterpassord som du er i stand til å huske, og tilpass dette passordet til de forskjellige webområder. Først må du velge et godt masterpassord som inneholder mer enn seks tegn, og som er en kombinasjon av bokstaver og tall (i stedet for faktiske ord). La oss i dette eksemplet bruke frasen "miffli8n". Deretter legger du til første og siste bokstav fra navnet til webområdet du skal ha passord til. Hvis dette er Amazon.com blir eksemplet "Amiffli8n". Sånn blir det enklere å huske alle de forskjellige passordene og likevel la de være vanskelig nok til at de vil gi hackere store problemer. Sekvensen gir mening for meg, men ikke for noen andre. Det hjelper også at jeg får forskjellige passord for forskjellige kontoer. For hvis passordet til en konto er røpet, vil de andre likevel være sikker.

Det blir bare flere og flere passord! Og det ene er mer komplisert enn det andre. Alle har vanskeligheter med å holde orden på dem og hente frem det riktige når det trengs. Så hvordan administrerer du dem? Det finnes noen programvarer som administrerer passord, og noen nettlesere kan lagre passordene. Det er veldig usikkert å ha alle passordene på en liste på datamaskinen, på papir ved siden av datamaskinen osv. En merknad til foreldre – sørg for at dere har tilgang til barnas passord til e-postkonto, direktemeldingskonto og kontoer på sosiale nettverkssider. Dette er en god ide fordi du kan finne ut hvem det er som kommuniserer med barna dine, og i tilfellet det skulle oppstå problemer, har du tilgang.

Sikre ditt trådløse nettverk

Trådløse hjemmenettverk byr på egne sikkerhetsproblemer, og du kan følge noen enkle trinn for å sikre at nettverket er trygt mot utenforstående inntrengere som vil bruke din båndbredde eller i verste fall utnytte ditt hjemmenettverk til utsendelse av spam eller angrep mot utenforstående. Dessuten vil et trådløst nettverk gjøre det mulig for barna å komme på nettet over alt i boligen, og dette kan undergrave dine forsøk på å holde deg informert om deres Internett-aktiviteter.

Hvis du har trådløst system hjemme, bør du sørge for at det er sikret: Tilbakestill ruterens passord slik at følger gode regler for passord og ikke er lett å gjette seg til, aktiver trådløs kryptering for å blokkere for fremmede som finner ditt nettverk på Internett, begrens tilgangen systemet ditt deler på nettverket og sørg for at ditt sikkerhetsprogram for Internett er oppdatert. Noen foreldre kobler til og med fra ruterens og tar dem med seg på soverommet når de går og legger seg.

Foreldrekontrollprogramvare

Foreldrekontrollprogramvarer gir deg mulighet for å velge hvor barna kan gå online og sikrer at de ikke ser upassende innhold.

Foreldrekontrollsystemer er forskjellige avhengig av hvilke program som tilbyr funksjonen. Det eksisterer som oftest forskjellige nivåer, slik at du kan tilpasse programmet i forhold til barna som skal beskyttes. For en femåring er det en god ide å opprette en liste over forhåndsvalgte foreldregodkjente webområder som du tillater barnet å besøke. Eller du kan opprette en konto hvor det kreves pålogging fra foreldrene for at barnet skal kunne surfe, eller en tidsbegrensning

slik at barna ikke bruker timevis på nettet i stedet for på leksene eller andre aktiviteter.

Eldre barn og tenåringer kan gis mer tilgang og fleksibilitet. Du kan begrense nettilgangen etter kategori i programmets bibliotek, for slik å hindre at barna utsettes for rasistisk, pornografisk eller annet upassende innhold.

Men husk at ingen programmer gir perfekt beskyttelse. Foreldre må bruke en kombinasjon av verktøy og regler for å beskytte barna, uansett deres alder. Internett er en rik informasjonskilde, og det vil ikke tjene formålet å lukke for det helt. Det er nødvendig at foreldre snakker med sine barn for å sikre seg at barna forstår foreldrenes verdier når de er på Internett.

Internett-favoritter

Sosiale nettverkssider som MySpace, Facebook og Bebo er veldig populære blant tenåringer. YouTube er populær, men også en bekymring for foreldre fordi den ikke har noen filtrering for språk og upassende innhold. Sjekk med skolen hvilke sider som er mest populære. Spør dine tenåringer om de har kontoer (men forsøk alltid selv å sjekke). Yngre barn besøker og melder seg inn på hobby sider som Stardoll og Barbie. Dette er webområder som tilbyr spill og forskjellige andre aktiviteter, inkludert chat. De fungerer på mange måter som andre sosiale nettverkssider, om enn som lettere utgaver.

Undervisningssider hjelper barna med lesing og matematikk. Enten barna dine er tenåringer eller yngre, så spør dem alltid om hvilke sider som er mest populære blant dem og deres venner. Spør dem hvilke sider de har registrert seg på, og la dem vise deg rundt på siden. Du vil raskt oppdage om du synes siden er OK eller ikke. La samtalen være uhytidelig, slik at barna ikke føler de blir forhørt.



Risiko

Overgripere på Internett

Selv om det er sjeldent at barn kommer i kontakt med seksuelle overgripere på nettet, så er det mange nok eksempler med tragisk slutt til å gjøre foreldre urolige. Sørg for at barna vet at de aldri må kommunisere med fremmede via e-post, chatting eller tekstmeldinger. Det er aldri OK å møte fremmede, verken på eller utenfor nettet. Sørg for at de forstår at selv om de møter noen på Internett, så er de likevel FREMMEDE, uansett hvor ofte de har kontakt på nettet. Det har vist seg at barn som diskuterer sex med fremmede på Internett er mer åpen for å arrangere møter ansikt til ansikt enn andre. Det er veldig viktig at du forteller dine barn at det aldri er akseptabelt å snakke om sex med fremmede på Internett, og at de må gi deg eller andre voksne som de kjenner, beskjed om dette hvis det skjer.

Plagiat og lureri

Det er lett å finne lekseveiledninger på nettet for alle de mest brukte lærebøkene, og mange webområder tilbyr stiler og andre skriveoppgaver for salg. Det har aldri vært så lett å fuske som i dag, og det kan være en stor fristelse for barna. Det er derfor viktig å forklare barna forskjellen mellom å bruke Internett når man gjør lekser, og å kopiere direkte fra Internett. Fortell dem at det er en god ide å kontrollere kildene til informasjonen som de har funnet på Internett, og forklar dem at brukergenererte webområder, som Wikipedia, kan være et fint sted å finne informasjon, men den er ikke alltid pålitelig. Informasjon funnet på Internett, bør kontrolleres opp mot mer tradisjonelle informasjonskilder, som leksikon.

Nettmobbing og nettfølgelse

Teknologi gir barna flere muligheter til å sosialisere og kommunisere og være i kontakt med hverandre enn noen gang. Dessverre bruker noen barn e-post, direktemeldinger og mobiltelefonbilder og tekstmeldinger til å mobbe andre barn. Dessuten kan barns digitale meldinger redigeres slik at meningen endres, og deretter sendes de videre til andre barn, bare for å gjøre det pinelig for offeret.

Gjør barna oppmerksom på at de må passe på selv de mest vanlige tekstmeldingene og tenke seg om når de skriver dem. De bør aldri ta igjen ovenfor nettmobbere med samme mynt og bør alltid fortelle deg hvis og når de blir nettmobbet. Gjem en kopi av mobbemeldinger ved å benytte "Print Screen"-tasten (kopierer skjermbildet) på datamaskinens tastatur og lim det deretter inn i et Word-dokument. Det er viktig at barna vet hvor de skal henvende seg for å rapportere nettmobbing.

Nettfølgelse, eller "cyberstalking", er en farlig utvikling av nettmobbing og utføres av dem som driver med følgelse i den virkelige verden utenfor Internett. Hvis eldre tenåringer er bevisst fenomenet, kan de bedre beskytte seg selv, og foreldrene bør vite hvordan de skal kunne hjelpe. Følgere eller stalkerne kan f.eks. kidnappe en e-postkonto og late som han eller hun er den personen som eier kontoen. En angriper kan ødelegge en sosial nettverksside eller sende hatmeldinger til offerets venner, foreta identitetstyverier eller forsøke å ødelegge noens kreditt eller rykte. Nettfølgelse er farlig og bør anmeldes til politiet, Internett-leverandøren og webområdeverten. Gjem alle beviser både når det gjelder nettfølgelse og nettmobbing.

Deling av filer, musikk og video

Barna lærer raskt gleden ved å dele musikk med hverandre. Og det er ofte barn i 8–12-årsalderen som finner frem til fildelingssider, hvor de kan bytte musikk og film på Internett. Forklar barna farene ved å besøke sider og programmer som benyttes til å dele filer, og at dette gir fremmede tilgang til datamaskinen. Hvis du bruker fildelingssider, kan dette utsette datamaskinen og dataene for bot-programmer, spionprogrammer, tasteloggere, virus og annen ondsinnet kode. Dessuten er det ofte ulovlig å laste ned musikk og video. Vis barna hvor de kan laste ned musikk og video lovlig, fra sider som iTunes.

Tyveri av identitet og informasjon

Mange barn vet ikke hva "privat" informasjon er for noe, og at det er viktig at disse forblir private både online og offline. Derfor er det viktig at du forklarer barna at private data er alle data som kan identifisere dem og gjøre det mulig for fremmede å stjele personlig eller økonomisk informasjon. Privat informasjon inkluderer data fra den virkelige verden, navn, telefonnumre, adresser, navn på idrettslag, skoler, fastlege osv. Svindlere kan bruke selv de minste spor til opprette en full profil for barn og foreldre. De selger så disse private dataene for å tjene penger. Det er overraskende enkelt for folk med slike intensjoner å søke om kreditt i dine barns navn og motta virkelige varer og penger, samtidig som de ødelegger ditt barns (eller din) kredittverdighet og gode navn.

Hvis du har mistanke om at barnet ditt er et offer for identitetstyveri, bør du overvåke dine kontoutdrag for å se etter merkelige endringer. Hvis du finner beviser for identitetstyver, må du rapportere dette til myndighetene og du bør i første omgang ta kontakt med politiet lokalt. Politirapporten vil styrke din sak når du arbeider med andre webområder og virksomheter som er involvert. Du kan også "låse" din og dine barns kredittrapport.

Sosiale nettverkssider

Sosiale nettverkssider er blant de mest populære fenomenene på Internett for barn, ungdom og voksne, men det er mest populært blant eldre barn og tenåringer. Blant de mest populære sosiale nettverkssidene er MySpace, Facebook and Bebo. De er alle steder hvor barn kommer sammen online og møter nye og spennende venner. Når det brukes med fornuft, er dette en god måte for barna å kommunisere og dele deres opplevelser. Men hvis de brukes uforsiktig, kan de utsette barna for identitetstyveri og overgrepere.

Lær barna at de må stille sine profiler til privat, slik at kun inviterte venner kan se informasjonen deres. De må ikke poste private data eller upassende eller villedende bilder. Når slik informasjon først er postet, er de offentlige og kan lastes ned og lagres på andres datamaskiner. Selv om du fjerner informasjonen eller bildene, kan de likevel dukke opp igjen på Internett og da kan de være under andres kontroll.

Sosiale nettverkssider gjør det mulig for barn å danne vennenettverk

som kan kommunisere med hverandre. Sørg for at barna ikke tillater folk som de ikke kjenner å bli med i deres nettverk. Når fremmede først er kommet inn i nettverket, vil de andre i nettverket til en viss grad stole på dem, fordi de stoler på dem som slapp dem inn. Hvis de fremmede er overgripere, kan de utnytte barna på nettverket.

Sørg for at dine barn setter kommunikasjonsegenskapene slik at de kan godkjenne alt som kommer til deres side. Dermed kan ikke engang en god venn poste pinlige, men morsomme bilder eller komme med meldinger du helst ikke vil se på siden.

Porno, spill, rasisme, anoreksi og hat på nettet

Nettets mørke hjørner inneholder noen farlige og ulovlige elementer. Uten foreldrekontroll eller nettleserfiltre er det nesten ikke til å unngå at barna vil møte noe som du og de vil synes er ubehagelig. Sørg for at dine barn vet at de kan komme til deg hvis noe slikt skjer og forsikre dem at du ikke blir sint.

Enkelte barn og tenåringer kan være nysgjerrige når de møter sider med rasistisk eller hatefullt innhold eller sider som er anoreksifremmende eller på andre måter selvdestruktive. Dette kan du kun oppdage hvis du jevnlig sjekker datamaskinens nettleserlogg. Selv ett enkelt besøk bør være nok at du snakker med barnet om det. Ikke anta at det var harmløs nysgjerrighet. Forklar reglene dere har i huset om slike webområder, og spør barna om hvorfor de besøkte sidene. Hvis barnet røper problemer som depresjon og dårlig selvbilde når det konfronteres med dette, bør du straks ta kontakt med fagfolk.

Online privatliv for tenåringer

Lær tenåringene om Internett. Nå er de gamle nok til å ha vett til å vite (eller bør ha det) at alle folk på nettet er ikke hva de gir seg ut for å være. På Internett er det lett å lyve om alder, kjønn og sted, og mange mennesker gjøre det av uskyldige eller ikke så uskyldige årsaker. Det er viktig hele tiden å understreke ovenfor dine tenåringer at man ikke kan stole på fremmede online, akkurat som man heller ikke kan stole på fremmede man møter ansikt til ansikt. De bør aldri gi fremmede lov til å komme på en venneliste eller delta i en chat. Og de må aldri akseptere gratis programvarer, ringetoner eller skjerm-sparere fra fremmede.

Minn din tenåring om at e-postadresser, brukerkontonavn og avsendernavn på direktemeldinger aldri må inneholde deres virkelige navn eller navnet på deres skole eller en kombinasjon av disse. Videre bør slike navn verken være eggende eller på andre måter kunne tiltrekke seg overgriper. De bør være så anonyme som mulig. Dessuten bør de aldri dele passord, selv med venner.

Kontroller at barnas skolewebområder er passordbeskyttet eller krever pålogging hvis man ønsker mer enn overfladisk offentlig informasjon. For eksempel benytter mange skoler i dag webområder til å kunngjøre reisepålegg og lister med navn på dem som skal reise på skoletur. Det sier seg selv at dette er informasjon som ikke bør ligge offentlig tilgjengelig.

E-post og direktemeldinger

Sørg for at barnas e-postadresse har det høyeste nivå aktivert på spamfilteret. Ifølge en Symantec-undersøkelse sier 80 % av barna som ble spurt, at de mottar upassende spam hver dag. De bør bruke e-postadresser som ikke kan gjøre det mulig for fremmede å spore dem opp. F.eks. bør de ikke bruke kombinasjoner med fornavn og etternavn. De bør heller ikke bruke assosiasjonsskapende navn eller adresser, som "sexylexy" eller "wildthing", selv om de synes det er litt kult å gjøre det.

Sørg for at de bruker sterke passord som de aldri deler, selv med venner. Du bør kjenne passordet til barnas e-postkontoer, slik at du har mulighet for jevnlig å kontrollere deres aktiviteter. Se hvem de sender e-post til og mottar dem fra. Kjenner du alle sammen? Og husk å la dine barn vite at du gjør dette for å beskytte dem, og ikke fordi du ikke stoler på dem.

Viktige anbefalinger:

- Lær barna at de ikke skal klikke på koblinger i e-poster som de mottar, fordi koblinger kan føre til falske webområder.
- Deaktiver forhåndsvisning i e-post. Dette hindrer at potensielle ondsinnede koder i meldinger går automatisk i gang.
- Barn bør ikke svare på e-post eller direktemeldinger fra noen som de ikke kjenner eller forventet å motta meldinger fra.
- Aksepter aldri en kobling eller å laste ned en fil via direktemeldinger.
- De bør ikke offentliggjøre sine direktemeldingsprofiler eller sosiale nettverkssider.

- Innstillingene for direktemeldinger bør stilles slik at de holder fremmede unna.
- De bør ikke tillate sider å vise når de er online eller å vise deres ID eller annen privat informasjon på sidene som de besøker.
- De bør alltid logge ut når de ikke bruker direktemeldinger, eller når de redigerer deres sosiale nettverksside, for slik å beskytte sitt privatliv.

Blogging

En blogg er en online journal eller dagbok. Noen er emnebaserte og viet et spesielt tema. Ofte har tenåringer blogger som ligner mer på tradisjonelle dagbøker, bortsett fra at de kan leses av alle. Ved å legge bloggen på eget web område eller sosial nettverkside er det samme som å publisere dagboken med verdensomspennende distribusjon. Barna bør vite hva de skal bruke bloggen til før de blogger. Søkemotorer kan vanligvis fiske opp informasjon som allerede er lagt ut på nettet, så da er det ikke så mye du kan gjøre for å beskytte privatlivet ditt. Hvis du laster opp bilder eller koblinger til private webområder på bloggen, er dette også med på å redusere privatlivet.

I tillegg kan potensielle arbeidsgivere eller skoler lese din blogg og dette kan ha konsekvenser for fremtiden din. F.eks. har folk i jobbintervju fått avslag pga. ting som har stått i bloggene deres eller i familie og venners blogger, hvor de er nevnt. Ikke la barnet ditt bli et bloggoffer.

Virus, ormer og spionprogrammer

Datavirus har i forskjellige former vært kjent i mer enn 25 år. Men det var først da det ble populært med e-post og fildeling at distribusjonen av disse truslene virkelig tok av. De som lagde virus eller andre former for ondsinnet kode eller "malware" gjorde dette for å lage så mye skade som mulig, for å vise programmeringstalentet sitt til hverandre. Men i dag er det mye mer på spill og mange av de internasjonale nettkriminelle er motivert av økonomisk vinning.

Ondsinnede koder som spionprogrammer, tasteloggere og boter kan gjøre stor skade når de distribueres via e-post, direktemeldinger, infiserte sosiale nettverkssider og fildelingssider. Spionprogrammer og tasteloggere overvåker dine normale aktiviteter på datamaskinen og rapporterer dine private data via Internett til kriminelle. Boter (forkortelser for "roboter") er programmer som kan snike seg inn i datamaskinen og få den til å sende ut spam og phishing-e-post til andre, uten at du vet det.

Beskytt barna og datamaskinen ved å installere Internett-sikkerhetsprogramvarer på familiens datamaskiner og sørg for at programmet er oppdatert med de siste beskyttelsesfilene. Fortell barna at de ikke må deaktivere virussøk eller brannmuren, selv om de tror dette vil gjøre spillet raskere. Risikoen er ganske enkelt for stor.

Bot på alvor

En "bot" er en form for ondsinnet programvare plassert på datamaskinen av nettkriminelle, og som gjør det mulig for angripere å overta kontrollen av den infiserte datamaskinen. Disse nettrobotene er vanligvis en del av et nettverk med infiserte maskiner som brukes til å gjennomføre en rekke forskjellige automatiske angrep, som spredning av virus, spionprogrammer, spam og andre ondsinnede koder. Ikke nok med det. Boter er også i stand til å stjele dine personlige data og skade din kreditt ved å blant annet bruke dine kredittkort og bankkontoer.

Botene kan også vise falske webområder, fremstå som legitime og lure deg til å overføre penger og oppgi brukernavn og passord som så brukes i kriminell virksomhet. Den beste beskyttelsen mot boter er å installere gode sikkerhetsprogrammer og sørge for at du setter opp programmene slik at de oppdateres automatisk slik at du får det siste nye innen beskyttelse.

Digitale bilder

Mange barn har mobiltelefoner med kamera, og mange har sitt eget digitalkamera. Snakk med barna dine om at det er viktig å beskytte bildene mot fremmede på nettet, og til og med fra venner som kan bruke bildene på en upassende måte. Du kan spore sending av digitale bilder fra telefonen (se kontoutskriftene). Sørg for at barna viser deg bildene som de har liggende på telefonen, slik at du kan gi dem råd hvis det er noen av dem du mener de ikke bør dele (fordi det er upassende eller risikofylt). Hvis du benytter fotodelingssider som Flickr, bør du innstille dem slik at ikke andre kan bruke bildene dine, spesielt hvis det er bilder av mennesker.

Viktige anbefalinger:

- Ikke offentliggjør private fotoalbum.
- Krev passord av dem som vil se bildene på en fotodelingsside.
- Sikkerhetskopier bilder med sikkerhetskopieringsprogrammer, for datamaskiner kan bryte sammen, og strømsvikt og naturkatastrofer kan slette bildene og andre datafiler.
- Bruk bare online fototjenester som tilbyr beskyttelse.
- Hvis du på en fotodelingsside kan sende e-post via siden til venner, er det bedre at du sender dine venner en kobling til siden i stedet for.

Internett-handel

Internett er en shoppers paradisi, spesielt for tenåringer med et kredittkort eller et forhåndsbetalt gavekort. Men det finnes regler for sikker shopping. Begynn Internett-shopping med å sjekke at sikkerhetsprogramvaren er aktivert og oppdatert. Shop kun på kjente og vel ansette sider, for å handle på et ukjent webområde kan være risikofylt. En måte å øke sikkerheten på er å sørge for at sider hvor du gir fra deg personlig informasjon (så som passord eller kredittkortsnummer) bruker kryptering. Krypterte nettadresser starter med "https". Du kan også sjekke om hengelåsikonet på nettleserens grunnlinje vises, noe som indikerer at webområdet du besøker, benytter kryptering for å beskytte kommunikasjonen med dem som besøker siden.

Shopping på vel ansette sider er første trinn til sikker Internett-shopping. Klikk aldri på koblinger i e-poster for å komme til en nettbutikk eller et salg. Du bør skrive inn butikkens adresse i nettleseren. Dermed unngår du faren for å bli et offer for phishing-

angrep, hvor du vil bli sendt videre til et falskt webområde som ligner den siden du vil handle på. Phishere kan stjele passord, påloggingsinformasjon, kredittkortinformasjon og det som verre er.

Sjekk kontoutskrifter for kredittkort så ofte som mulig, minst én gang i måneden. Dette er den beste måten å kontrollere om det er noen som bruker kredittkortet, og å oppdage problemer før de blir vanskelige å løse. Kredittkortselskaper tilbyr kundene beskyttelse og vil samarbeide med deg angående tvister eller uautorisert bruk.

Nettbanktjenester

Hvis du eller ditt barn benytter en nettbanktjeneste, må dere aldri gjøre dette på en offentlig eller delt datamaskin eller på et trådløst nettverk som mangler sikkerhetsfunksjoner som f.eks. en brannmur. I så fall risikerer du at en hacker fanger opp konto- og påloggingsinformasjon og stjeler pengene dine. Skriv alltid inn nettadressen til din bank i nettleseren, klikk aldri på en kobling i en e-post.

Internett-spill og tegn på avhengighet

MMORPG – hva er det? Det er forkortelsen for en populær og potensielt sett avhengighetsskapende form for Internett-spill og står for "Massive multiplayer online role-playing games". Titler som World of Warcraft, Lord of the Rings og Everquest er blant de mest populære i dag. Dette er spill som det er veldig lett å bli oppslukt av, spesielt for mange gutter blir disse spillene en ren besettelse. Gi barna regler for hvor mye tid de kan bruke på disse sidene, om de får eller ikke får penger som de kan bruke til å betale medlemskap eller kjøpe spilltilbehør (i den virkelige verden eller i selve spillet) og for andre ting du er bekymret for. Tegn på Internett-spillavhengighet ligner på tegn på avhengighet i den virkelige verden. F.eks. at de lengter etter å spille, at de blir innesluttet og asosiale, at de mister kontrollen og begynner å forsømme andre aktiviteter og oppgaver.



Noen ord avslutningsvis

Internett er en fantastisk ressurs hvor man ofte kan handle og føle som om man var på et virkelig sted. Internett tilbyr utdanning, underholdning, nyheter fra hele verden, og forbedrer våre liv med tjenester som chat, e-post, Internett-shopping og mye mer. Ved å få innsikt i de farer som kommer med å være på Internett, og ved å bruke oppdaterte sikkerhetsprogrammer, kan du hjelpe dine barn med å finne frem i denne utrolige nettverdenen på en trygg og uavhengig måte. Fortsett med å holde deg selv orientert ved å lære om ny teknologi og Internett-problematikk. Sørg for at din Internett-atferd er et forbilde for dine barn.

Gode råd for beskyttelse av familien på nettet:

- Plasser datamaskinen i familiens oppholdsrom.
- Opprett regler for bruk av Internett.
- Forstå sosiale nettverk.
- Lær dine barn å holde sin personlige informasjon beskyttet.
- Beskytt barnas passord.
- Kontroller jevnlig datamaskinens Internett-logg.
- Bruk tid sammen med barna på Internett.
- Lær dine barn om Internett-etikk.
- Vær datasmart.
- Lær dine barn å fortelle sine foreldre, lærere eller andre voksne dersom de føler seg ukomfortable med noe de har sett på Internett.

Viktige ressursider

www.nettvett.no

www.saftonline.no

www.reddbarna.no

www.barnevakten.no

www.tryggsurf.no

Hvis du ønsker den nyeste informasjonen om
kommende Internett-trusler eller hvis du vil abonnere på nyhetsbrevet
Internett-sikkerhet for familien
Gå til **www.symantec.no**

INGEN GARANTI. Denne informasjonen leveres til deg som den er, og Symantec Corporation kan ikke garantere for informasjonens nøyaktighet eller bruk. All bruk av dokumentasjonen eller informasjonen i dette dokumentet skjer på brukers egen risiko. Dokumentasjonen kan inkludere tekniske eller andre unøyaktigheter eller typografiske feil. Symantec Corporation forbeholder seg retten til å gjøre endringer uten forhåndsvarsel.

Copyright © 2008 Symantec Corporation. Med enerett. Symantec og Symantec-logoen er varemerker eller registrerte varemerker for Symantec Corporation eller dets tilknyttede selskaper i USA og andre land. Andre navn kan være varemerker for deres respektive eiere.