

OUCH!

I DENNE UDGAVE...

- Baggrund
- Det grundlæggende
- Børn

Sikring af familien

Baggrund

Mange af os føler os trygge ved ny teknologi og ved hvordan vi kan bruge den sikkert. Men du har sikkert familiemedlemmer der ikke lige så trygge, specielt hvis de ikke er opvokset med computere og internettet. I dette nyhedsbrev præsenterer vi en række handlinger du kan udføre for at hjælpe med at sikre dine familiemedlemmers teknologi. Måske gør du allerede noget for at sikre dine børn i dit eget hjem, men de samme forholdsregler findes sandsynligvis ikke når børnene besøge familiemedlemmer. Vi vil derfor også give forslag til, hvordan du kan sikre dine børn når de besøge familiemedlemmer.

Gæsteredaktør

Brian Honan (Twitter [@brianhonan](#)) er en selvstændig konsulent fra Dublin, Irland. Han har grundlagt og leder Irlands første CERT, er rådgiver for Europols Cybercrime Centre (EC3) og giver forelæsninger i informationssikkerhed ved University College Dublin. Han er forfatter til en række bøger og skriver for flere forskellige branche publikationer.

Det grundlæggende

Blot nogle få simple handlinger kan hjælpe meget med at gøre alles digitale liv sikrere. Disse anbefalinger gælder alle, men ikke alle forstår vigtigheden af dem. Hvis du har familiemedlemmer som ikke forstår hvorfor det er så vigtige at beskytte sig på nettet, så er det en god ide at snakke det igennem med dem.

- **Social manipulation:** Forklar hvad social manipulation er, i et sprog som er let at forstå. Svindel og bedrag er ikke noget nyt og har altid eksisteret; det eneste der er nyt er, at svindlerne nu benytter sig af internettet. Fortæl om de meste kendte typer svindel i dag, fx phishing forsøg, så som e-mails der udgiver sig for at være fra Skat eller telefonopkald fra "Microsoft kundeservice" hvor en person beder om adgang til en computer. Sørg for at alle forstår, at de aldrig må udlevere kodeord eller give folk de ikke kender adgang til at fjerne styre deres computer. Endelig, og måske vigtigst af alt: Sørg for at alle ved, at hvis de er i tvivl om det er OK at åbne en e-mail eller aflevere oplysninger i telefonen eller på internettet, så kan og bør de altid spørge dig til råds!
- **Wi-Fi i hjemmet:** Sørg for at hjemmets Wi-Fi er sikret korrekt. Som et minimum bør du sørge for at der benyttes den seneste kryptering, samt at kodeord er skifter fra fabriksindstillingerne. Der vil næsten altid være to kodeord der skal skiftes: Administrator kodeordet til at logge direkte ind på routeren, samt det kodeord der bruges til at logge på Wi-Fi forbindelsen. Sørg for at bruge stærke kodeord eller kodesætninger. Det er også muligt at benytte sig af en sikker form for DNS, så som www.opendns.org. Sikker DNS som denne forhindre

Sikring af familien

ikke folk i at besøge inficerede hjemmesider, men kan give dig kontrol over hvilke sider man kan besøge, hvilket kan være godt når børnene er på besøg.

- **Opdateringer:** At holde systemer opdaterede, er et af de mest grundlæggende tiltag du kan gøre for at holde computere og enheder sikre. Sørg for alle enheder (inklusiv mobiltelefoner) og applikationer er fuldt opdaterede. Når det er muligt bør du altid slå automatisk opdatering til.
- **Anti-virus:** Der vil altid ske fejl; nogle gange kommer man til at installere noget som man ikke skulle have, eller klikke på den e-mail som man ikke skulle have åbnet. Det er derfor vigtigt at have et anti-virus program installeret på alle computere, samt at det er opdateret og aktivt!
- **Kodeord:** Når man taler om at beskytte konti og enheder kan man ikke komme udenom kodeord og du bør forklare dine familiemedlemmer, hvordan man laver et stærkt kodeord. Kodesætninger er sikkert både det nemmeste og letteste for dem at huske og bruge. En anden ide er at installere et program til at gemme kodeord (og lære dem at bruge det), eller alternativt at skrive kodeordene ned og gemme dem et sikkert sted, som kun de har adgang til. Sørg for at slå totrinsbekræftelse til på vigtige hjemmesider og konti. I Danmark er vi så heldige, at alle banker og offentlige institutioner skal bruge Nem-ID, så vi behøver ofte ikke selv at slå totrinbekræftelse til der. Bemærk dog, at mange banker ikke kræver totrinsbekræftelse for at se dine oplysninger. Det betyder, at hvis dit kodeord til Nem-ID bliver stjålet eller gættet, så kan kriminelle se dine bankoplysninger på nettet. Det er derfor stadig vigtigt med gode kodeord!
- **Backup:** Når uheldet er ude, så kan en god backup redde dagen. Sørg for at alle familiemedlemmer automatisk tager backup og at de jævnligt sikre sig at backuppen virker.



Ældre generationer har ofte brug for hjælp til at sikre teknologi i deres hjem og til at skabe et sikkert teknisk miljø for besøgende børn.

Hvis du vil være sikker på at tingene fungerer som de skal, er der ikke andet at gøre end at checke det med jævne mellemrum, fx en gang om måneden eller i kvartalet. For at gøre det lettere, kan det være nødvendigt at installere software der kan give dig fjernadgang til familiemedlemmers computere, men hvis du gør det, så sørg for at det er sikret med både stærk kryptering og et unikt, stærkt kodeord.

Børn

Når børn besøger deres bedsteforældre, har de regler, som gælder der hjemme, det med at blive blødt lidt op eller

Sikring af familien

forsvinde helt, inklusiv regler som er lavet for at beskytte børnene på nettet. Her er nogle forslag til hvad du kan gøre for at beskytte børnene når de besøger andre.

- **Regler:** Hvis du har opsat regler der har til formål at beskytte børnene på nettet, så bør du sørge for at bedsteforældre og andre som børnene besøger kender til dem. Hvis der for eksempel er regler for hvor ofte børnene må spille på nettet eller sidde med deres mobiltelefoner, så sørg for at disse regler følger med børnene når de besøger andre familiemedlemmer. Det er højst usandsynligt at børnene selv forklarer reglerne når de kommer ud, så det er op til dig. En måde at gribe det an på er at have en liste med regler som du kan give ud.
- **Kontrol:** Hvis børnene forstår teknologien bedre end deres bedsteforældre eller andre de besøger, så kan de i nogen tilfælde udnytte det. De kan for eksempel få administrative rettigheder på bedsteforældrenes computer og installere det spil de ikke må spille eller lignende. Sørg for at dine familiemedlemmer ved at de ikke bør give børnene forhøjede rettigheder til systemerne.

Læs mere

Besøg os på <http://www.securingthehuman.org>, hvor du kan abonnere på det månedlige OUCH! nyhedsbrev om sikkerhedsbevidsthed, se ældre udgaver i OUCH! arkiverne og lære mere om SANS løsninger til at skabe bevidsthed om sikkerhed.

OUCH! er oversat af Jacob Vibe Hammer. Han arbejder til daglig som Software Arkitekt hos Kamstrup, hvor han arbejder med udvikling og sikring af Kamstrups Smart Grid løsninger.

Ressourcer

Social manipulation:	http://www.securingthehuman.org/ouch/2014#november2014
Sikring af dit hjemmenetværk:	http://www.securingthehuman.org/ouch/2014#january2014
Kodesætninger:	http://www.securingthehuman.org/ouch/2015#april2015
Beskyt dine børn på nettet:	http://www.securingthehuman.org/ouch/2013#april2013
Teknisk support svindel:	http://www.onguardonline.gov/articles/0346-tech-support-scams
Plakat om sikkerhed i hjemmet:	http://www.securingthehuman.org/resources/posters

Licensinformation

OUCH! udgives af SANS Securing the Human og distribueres under "[Creative Commons BY-NC-ND 3.0](http://creativecommons.org/licenses/by-nc-nd/3.0/)" licensen. Du er velkommen til at videregive nyhedsbrevet eller bruge det i dit eget bevidsthedsprogram, så længe du ikke ændre nyhedsbrevet. Du kan kontakte OUCH! på www.securingthehuman.org/ouch med spørgsmål om oversættelse eller andet.

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

Oversat af: Jacob Vibe Hammer



securingthehuman.org/blog



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



securingthehuman.org/gplus